SARUM HALL
SCHOOL

ONLINE SAFETY POLICY

Date:	September 2025
Next Review Due:	September 2027
Reviewed by:	Deputy Head (Academic & Innovation)

INTRODUCTION

At Sarum Hall School, online safety is a core element of our safeguarding and pastoral responsibilities. The purpose of this policy is to ensure that all members of the school community are aware of the risks associated with digital technology and the internet, and understand the measures in place to protect children and support responsible use. It provides a clear framework for managing online activity and promoting a safe, respectful and informed digital culture.

This policy applies to all members of the school community, including:

- Pupils (including EYFS children)
- Teaching and support staff
- Senior leaders and governors
- Volunteers and external visitors
- Parents and carers

It covers the use of school-owned devices and networks, personal devices used in school, remote learning environments, digital communication platforms, and all activity carried out online by or on behalf of the school.

This policy works alongside and should be read in conjunction with the following key documents:

- Child Protection and Safeguarding Policy – outlines the school's safeguarding procedures, including reporting concerns about online harm or exploitation.
- IT Acceptable Use Policy for Staff – sets out expectations for safe, professional use of school systems and communication.
- Taking, Storing and Using Images of Pupils Policy – provides guidance on the appropriate use of photography and videography within the school context.
- Data Protection Policy – outlines how personal and sensitive data is processed and protected, including in online environments.
- Behaviour Policy – includes expectations for online conduct and responses to cyberbullying or misuse.
- Anti-Bullying Policy – addresses bullying in all forms, including digital and online behaviour.
- Computing Policy – includes the provision for teaching digital literacy, online safety and responsible internet use through the curriculum.

This policy will be reviewed annually, or sooner if required by changes in legislation or statutory guidance such as Keeping Children Safe in Education (KCSiE).

RISKS AND HARMS

Online safety risks can be broadly categorised into four areas, commonly referred to as the '4 Cs': Content, Contact, Conduct, and Commerce. These categories help schools identify potential dangers and develop appropriate responses to protect pupils and staff.

- **Content** – being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
  Contact – being subjected to harmful online interaction with other users; for ample: peer to peer 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 – online behaviour that increases the likelihood of, or causes, harm; for example, 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, and
  Commerce – risks such as online gambling, inappropriate advertising, phishing and or financial scams. Incidents involving fraud or suspicious financial activity can be reported to the Anti-Phishing Working Group.

ARTIFICIAL INTELLIGENCE (AI)

The school recognises the growing role of artificial intelligence (AI) in education and is committed to ensuring its safe, responsible, and ethical use. Any AI tools used within the school must align with safeguarding requirements, data protection legislation, and the Department for Education's Generative AI: product safety expectations. Staff and pupils should be aware of potential risks linked to AI, including exposure to misinformation, disinformation, and inappropriate content.

AI is treated as part of the school's wider online safety provision and is subject to the same filtering, monitoring, and safeguarding oversight as other digital technologies. Staff receive training on emerging risks associated with AI, and pupils are supported to develop digital resilience and critical thinking when engaging with AI-based tools.

Further details, including expectations for staff and pupil use of AI, can be found in the school's separate Artificial Intelligence Policy, which should be read alongside this policy.

ROLES AND RESPONSIBILITIES

Online safety is a shared responsibility across the whole school community. Everyone who works with or supports children has a role to play in keeping them safe online.

Governing Body

The Governing Body holds strategic oversight of online safety in the school. Governors are responsible for:

- Ensuring there is a robust and up-to-date Online Safety Policy in place;
- Receiving regular updates on online safety incidents, training, and the effectiveness of filtering and monitoring systems;
- Ensuring that online safety is embedded within the school's safeguarding framework;
- Supporting the Headmistress in creating a culture of online safety across the school.

Safeguarding Governor

The Safeguarding Governor plays a key role in monitoring and supporting the implementation of online safety measures. Their responsibilities include:

- Meeting regularly with the Designated Safeguarding Lead (DSL) and Head of e-Learning who is also Deputy Head (Academic & Innovation) who is also to review online safety provision;
- Monitoring the delivery of staff training and pupil education related to online safety, ensuring these are in line with the policy;
- Participating in the annual review of the school's filtering and monitoring systems, alongside the Deputy Head (Academic & Innovation), DSL, SLT, and IT service provider, in line with DfE Filtering and Monitoring Standards;
- Checking that the school meets the DfE Cyber-Security Standards, using training and support to inform this oversight.

Headmistress and Senior Leadership Team (SLT)

The Headmistress has overall responsibility for implementing this policy and ensuring that online safety is embedded in the school's wider safeguarding culture. Responsibilities include:

- Treating online safety as a safeguarding priority and fostering a whole-school culture of vigilance and responsibility.
- Ensuring that clear, effective reporting procedures are in place, understood, and followed by all staff.
- Ensuring that online safety procedures are regularly reviewed and consistently applied.
- Ensuring that staff are trained to recognise, respond to and manage online safety risks appropriately.

- Ensuring the Designated Safeguarding Lead (DSL) and Deputy Head (Academic & Innovation) have the time, support and resources to fulfil their responsibilities and deliver training to colleagues as needed.
- Being aware, along with at least one other member of the SLT, of the correct procedures in the event of a serious online safety allegation against a member of staff.
- Overseeing the provision of internal online safety monitoring systems and ensuring that those responsible for monitoring (e.g. DSL, Deputy Head (Academic & Innovation), IT Support) receive appropriate support and oversight.
- Working in partnership with the DSL, Deputy Head (Academic & Innovation), IT Support and the responsible governor to ensure that filtering and monitoring arrangements meet DfE standards and are reviewed regularly.

Designated Safety Lead (DSL)

The DSL holds lead responsibility for online safety within their wider safeguarding role and works in close partnership with the Deputy Head (Academic & Innovation). Their responsibilities include:

- Leading the school's approach to online safety and ensuring it is fully embedded within the safeguarding framework and child protection procedures.
- Receiving regular, relevant training in online safety to stay informed about emerging risks, online trends, and digital threats.
- Holding up-to-date knowledge and the capability to support staff, advise pupils, and respond effectively to online safety concerns.
- Receiving and responding to online safety incidents logged via CPOMS, ensuring appropriate records are kept, actions are taken, and referrals to external agencies are made where necessary.
- Meeting regularly with the Safeguarding Governor to review anonymised incidents, discuss current risks, and examine filtering and monitoring logs.
- Ensuring that annual (or more frequent) checks of filtering and monitoring systems are conducted in collaboration with the Deputy Head (Academic & Innovation), SLT, IT provider, and responsible governor.
- Liaising with IT Support and relevant staff on matters related to online safety, digital safeguarding, and pupil welfare.
- Attending relevant governing body committees/meetings to report on online safety issues.
- Providing regular updates to the Headteacher and SLT on online safety matters, including incidents, patterns, training needs, and emerging risks.

Deputy Head (Academic & Innovation) (Online Safety Lead)

- The Deputy Head (Academic & Innovation) plays a key operational role in the implementation of the school's online safety strategy and works closely with the DSL to ensure that practice is effective, current, and proactive. Responsibilities include:

- Working in daily collaboration with the Designated Safeguarding Lead (DSL) to monitor and respond to online safety concerns.
- Receiving reports of online safety incidents, ensuring that all concerns are logged appropriately via CPOMS, and contributing to the ongoing review of incident trends to inform school strategy.
- Taking a lead role in the development, implementation and review of the school's online safety policy and related documentation.
- Conducting annual checks of the school's filtering and monitoring systems, in collaboration with the DSL, SLT, IT Support, and the Safeguarding governor, in line with DfE Filtering and Monitoring Standards.
- Promoting a culture of awareness and responsibility for online safety across the whole school community, including pupils, staff, parents/carers, and governors.
- Liaising with curriculum leaders to ensure the online safety curriculum is planned, mapped, embedded and evaluated effectively across subjects and year groups.
- Ensuring all staff understand the procedures for responding to online safety incidents and the importance of prompt and accurate reporting.
- Providing (or signposting) high-quality training and guidance on online safety for staff, pupils, governors and parents.
- Receiving regular training to stay informed about how digital technologies are evolving, particularly those used by pupils, and to understand the risk areas defined by Keeping Children Safe in Education (KCSiE).

IT Support (itsupport@sarumhallschool.co.uk)

The school's technical staff play a vital role in maintaining a secure and effective digital infrastructure that supports safeguarding and learning. They are responsible for:

- Understanding and following the school's Online Safety Policy to ensure that their work aligns with safeguarding expectations.
- Maintaining a secure technical infrastructure that is resilient to misuse, unauthorised access, and malicious attack.
- Ensuring the school meets or exceeds the DfE's technical requirements, as outlined in DfE Meeting Digital and Technology Standards in Schools & Colleges, and reflects any additional guidance from the local authority or governing body.
- Implementing safe and clearly managed systems of user access to school networks, devices, and cloud-based services.
- Staying up to date with developments in online safety, cybersecurity, and educational technology to support informed decision-making and risk mitigation.
- Monitoring the use of school technology effectively, flagging and reporting any misuse or attempted misuse to the Deputy Head (Academic & Innovation) for further investigation and action.
- Managing and regularly updating the school's web filtering system (SurfProtect by Exa Networks) to ensure harmful content is blocked appropriately.

- Maintaining and reviewing the school's monitoring system (Smoothwall by Qoria) to support safe and responsible use of school devices and networks.

Teaching and Support Staff

- All school staff have a responsibility to promote a safe and respectful digital environment and to model appropriate online behaviour. All staff must:
- Understand that online safety is a core part of safeguarding, and ensure their practice reflects current guidance, including Keeping Children Safe in Education.
- Have read, understood, and signed the Staff Responsible Use Policy for Devices and Emails.
- Be aware of current online safety issues, risks, and emerging trends, and stay up to date through regular training and internal updates.
- Immediately report any suspected misuse, breach, or safeguarding concern to the Deputy Head (Academic & Innovation) and/or DSL, following the school's safeguarding procedures and using CPOMS where appropriate.
- Ensure that all digital communication with pupils and parents/carers is professional, appropriate, and conducted only through official school systems.
- Supervise and monitor the use of digital technologies, mobile devices, and cameras during lessons and school activities, in accordance with school policies.
- Embed online safety teaching and digital responsibility into the curriculum and wider school life, ensuring pupils:
    - understand and follow the Online Safety Policy and the Pupil Responsible Use Agreement;
    - develop safe research skills and understand the risks of plagiarism and breaches of copyright;
    - know how to report concerns or inappropriate content.
- Pre-check websites and online resources used in lessons to ensure suitability, and have procedures in place to manage accidental access to inappropriate material.
- Uphold the school's zero-tolerance approach to all forms of online abuse, including cyberbullying, sexual harassment, discrimination, and hate-related content.
- Be alert to the role of technology in safeguarding and wellbeing concerns, such as sexting, grooming, radicalisation, and exposure to harmful content.
- Recognise that child-on-child abuse can take place online, as well as in physical settings.

  Model safe, responsible, and professional online behaviour, both within school and in their personal use of technology and social media.

Pupils

Pupils are expected to:

- Use the school's digital technology systems responsibly and respectfully, in line with the Pupils' ICT Responsible Use Policy and the Online Safety Policy.
- Follow the school's behaviour expectations when online, both in and out of school.

- Report any concerns about abuse, misuse, or access to inappropriate material to a trusted adult or member of staff.
- Know what to do and who to speak to if they or someone they know feels vulnerable, unsafe, or targeted when using online technology.
- Understand the importance of safe online behaviour beyond the school setting, and recognise that the school's Online Safety Policy may apply to their actions outside of school if they are related to their role as a pupil.
- Take part in the school's online safety education programme and apply their learning to their digital behaviour.

Parents and Carers

Parents and carers play a vital role in supporting children's online safety at home and in partnership with the school. The school will take every opportunity to help parents and carers understand online safety risks and how to manage them, through:

- Publishing the Online Safety Policy on the school website.
- Providing a copy of the Pupils' ICT Responsible Use Policy in school planners.
- Sharing clear guidance on the appropriate use of social media, particularly regarding posts about the school community.
- Requesting parental consent for matters such as the use of digital images, access to online learning platforms, and use of cloud-based services.
- Offering support through parents' evenings, newsletters, website updates, social media posts, and information about local and national online safety initiatives.

Parents and carers are encouraged to:

- Engage with school communications and updates on online safety.
- Monitor and support their child's use of digital technologies at home.
- Reinforce safe and respectful online behaviour as taught in school.
- Contact the school promptly if they have concerns about their child's online activity or wellbeing.

EDUCATION AND TRAINING

Pupils

Online safety is taught explicitly through the Computing and PSHE curriculum and is reinforced in assemblies, workshops, and enrichment activities. Lessons are age-appropriate and cover topics including online behaviour, cyberbullying, responsible use, and managing online risks.

Online Safety Curriculum

Online safety should be a focus across the curriculum, with staff reinforcing key messages in all subjects and settings where digital technology is used. The online safety curriculum

should be broad, relevant, and age-appropriate, providing opportunities for progression and creativity. It will be delivered in the following ways:

- A planned online safety curriculum is taught through both Computing and PSHE, and is regularly revisited and updated to reflect current risks and developments.
- Key online safety messages are reinforced during the school year through assemblies, form time/pastoral activities, and events such as Safer Internet Day/Week.
- The school appoints and trains Digital Leaders, who help to promote online safety among their peers and lead pupil-led initiatives.
- Pupils are explicitly taught to:
    - Understand the risks of sharing personal information and engaging with strangers online.
    - Recognise the signs of cyberbullying and develop strategies to respond safely.
    - Appreciate how their online reputation can be shaped by what they post or share.
    - Critically evaluate the content they find online and be aware of misinformation, fake news, and online hoaxes.
    - Understand how online content and social media can impact mental health, and how to seek advice or support.
    - Recognise and avoid the dangers of online challenges and harmful trends.
    - Acknowledge the sources of information they use and respect copyright and ownership of digital content.
    - Build resilience to radicalisation through the exploration of controversial issues in a safe, respectful environment.
- Pupils are supported in understanding and adhering to the Pupil ICT Responsible Use Policy, and are encouraged to apply safe and responsible behaviour both in and out of school.
- Staff model appropriate digital behaviour, using the internet and devices professionally and responsibly.
- In lessons where internet use is pre-planned, pupils are guided to teacher-checked, age-appropriate websites. Procedures are in place to respond if pupils access unsuitable material.
- Where pupils are permitted to use the internet more freely, staff remain vigilant and actively monitor pupil activity to ensure safety.

Staff

Al staff receive regular online safety training, including updates on safeguarding procedures, the Prevent Duty, and key changes to statutory guidance such as Keeping Children Safe in Education (KCSIE). Training now also covers recognising emerging online harms, such as misinformation, disinformation, conspiracy theories, and risks linked to generative AI. The school uses the Secure Schools online training platform to support staff development in areas such as phishing awareness, password protection, cyberbullying, safe classroom practice, and the psychological impact of online exposure. This platform allows for flexible,

role-specific training that is monitored and updated regularly to reflect new threats and responsibilities, supporting a whole-school culture of digital resilience and safeguarding.

Parents and Carers

The school supports parents and carers in keeping their children safe online by:

- Publishing the Online Safety Policy and guidance on the school website.
- Sharing the Pupil ICT Responsible Use Agreement in planners.
- Providing regular updates through newsletters, social media, and online safety bulletins.
- Hosting workshops, presentations, and signposting to national campaigns and resources.
- Offering clear guidance on social media use related to the school community.

FILTERING, MONITORING, AND SECURITY

The school has robust systems in place to safeguard digital activity and support safe, responsible use of technology. These include:

- Filtering through SurfProtect (Exa Networks) to block access to harmful or inappropriate content.
- Monitoring through Smoothwall (Qoria), which flags keyword concerns, browsing behaviour, and potential safeguarding issues for review.
- Secure access controls and strong password protection on all devices and platforms.
- Regular reviews of filtering and monitoring arrangements, conducted by the Deputy Head (Academic & Innovation), DSL, IT Support, and the Safeguarding Governor.
- It is recognised that, on occasion, pupils may need to access potentially sensitive content for legitimate educational purposes (e.g. topics such as racism, drugs, or discrimination). In these cases, staff may request that IT Support (or a designated person) temporarily lift filtering restrictions for specific, approved resources during the period of study.
- The school adheres to the DfE's Cyber Security Standards and Digital Technology Standards, ensuring that security systems remain up to date and fit for purpose.
- The school follows the UK Safer Internet Centre's Appropriate Filtering and Monitoring guidance, using a combination of strategies tailored to the school's risk assessment. These include:
  - Physical monitoring: Active adult supervision during classroom activities involving digital devices.
  - Internet use logging: Regular review and analysis of usage data and flagged activity.
  - Filtering log reviews: Regular analysis of SurfProtect filtering logs, with breaches reported to senior leaders.
  - Third-party assisted monitoring:
    - Apple Classroom for real-time monitoring of pupil activity on iPads.
    - Smoothwall for Chromebooks and Windows-based computers, supporting keyword and behaviour analysis.

- All concerns identified through filtering or monitoring are followed up in accordance with the school's safeguarding procedures and recorded on CPOMS where appropriate.
- Refer to the DfE's 'Plan Technology for Your School' tool to self-assess and improve filtering/monitoring setup.

RESPONDING TO ONLINE SAFETY INCIDENTS

Pupils

- All incidents related to online safety or the unacceptable use of technology by pupils must be recorded on CPOMS, with the Deputy Head (Academic & Innovation) alerted.
- If a pupil or member of staff accidentally accesses distressing, upsetting, or age-inappropriate content:
    - The screen should be immediately and calmly minimised or closed.
    - Staff should reassure pupils that they have done nothing wrong.
    - The incident must be reported to the Deputy Head (Academic & Innovation), including details of the website and its URL.
    - The Deputy Head (Academic & Innovation) will liaise with IT Support to ensure that access to the site is blocked and the filtering system is reviewed for effectiveness.

Device Checks (Where No Illegal Activity Is Suspected)

If there is a concern about online misuse that does not involve suspected illegal activity, device checks may be carried out following these procedures:

- One or more senior members of staff should be present during the process to ensure accountability and protect staff from future allegations.
- The investigation should be conducted using a designated school device, which is not used by pupils and, if needed, can be retained for potential police involvement.
- Staff carrying out the check must have appropriate authorised internet access. All sites visited and content viewed must be closely monitored and recorded.
- The URL(s) of any concerning sites must be logged, along with a brief description of the content.
- If necessary, screenshots may be captured and securely stored on the investigation device, in accordance with data protection procedures.
- Once the investigation is complete, the SLT, DSL, and Deputy Head (Academic & Innovation) will determine whether the concern is substantiated.
    - If so, appropriate action will be taken, which may include:
        - Internal disciplinary procedures;
        - Involvement of external agencies (e.g. police) where appropriate.

Safeguarding Incidents

Any incident that raises concerns about illegal activity or the potential for serious harm must be escalated immediately in accordance with the school's safeguarding procedures. This includes, but is not limited to, the following types of online-related harm:

- Non-consensual sharing of images
- Self-generated sexual images or videos
- Terrorism or extremist material
- Hate crime or abuse
- Online fraud or extortion
- Harassment or stalking
- Child Sexual Abuse Material (CSAM)
- Grooming and Child Sexual Exploitation
- Accessing or sharing extreme pornography
- Online sale of illegal materials or substances
- Cyber or hacking offences under the Computer Misuse Act
- Copyright infringement or digital privacy

Incidents Involving Sexualised Harms and Indecent Imagery

Any concerns relating to sexualised harms, including nude or semi-nude images shared between pupils—must be reported to the DSL immediately.

If a member of staff becomes aware that a nude or indecent image of a pupil has been shared:

- They must not intentionally view the image.
- They must never copy, print, share, store, or save any such content.
- If the image was viewed accidentally, this must be reported to the DSL, and appropriate advice must be sought.
- Staff must not instruct pupils to delete any content or images.
- In some situations, it may be appropriate to confiscate the device (without viewing the content) and pass it to the police to preserve potential evidence.

Staff must follow the guidance outlined in:

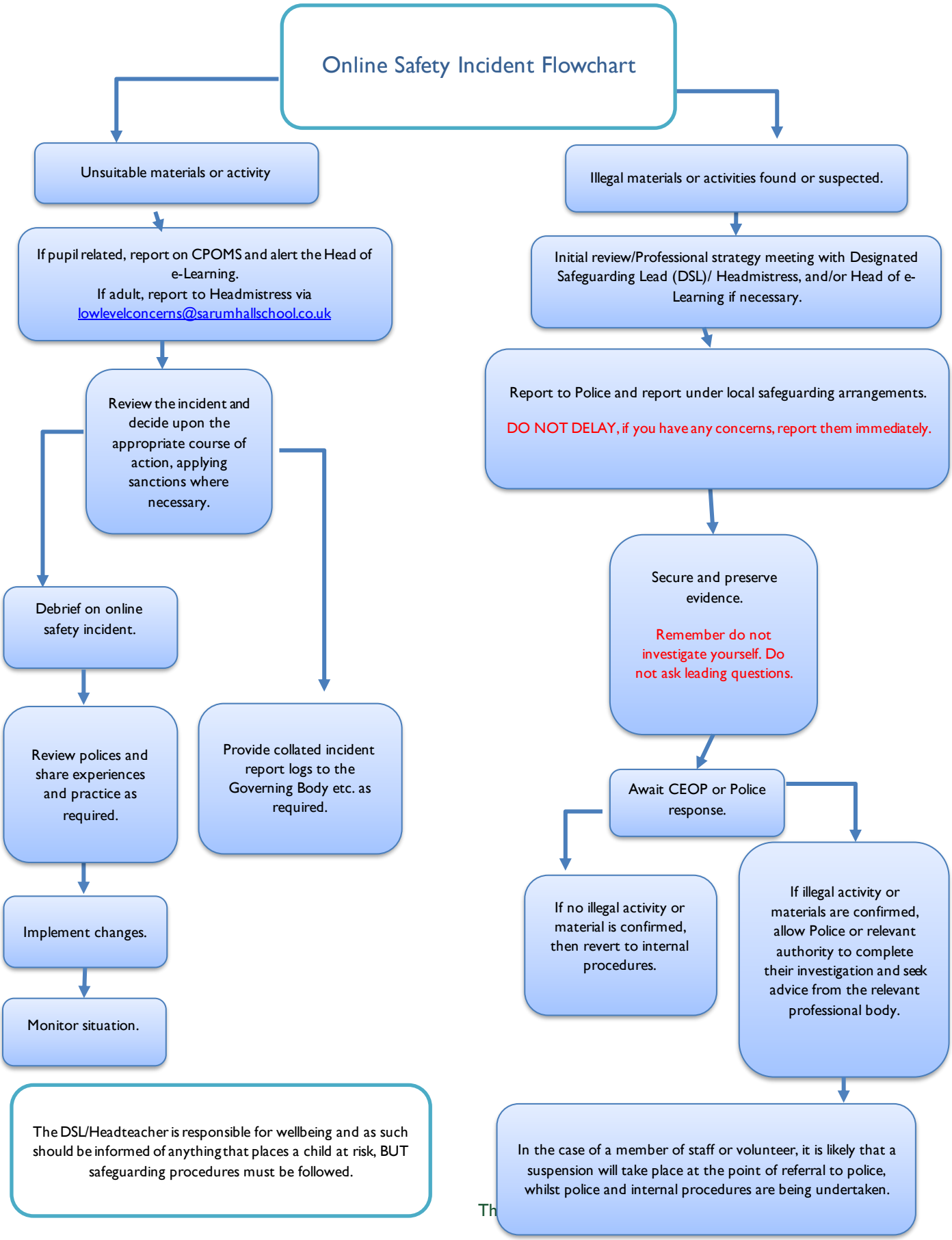
- Section 18 of the Child Protection and Safeguarding Policy
- The DfE's Searching, Screening and Confiscation guidance
- Government's guidance on Sharing Nudes and Semi-Nudes: How to Respond to an Incident

Staff Incidents

Any concerns regarding staff misuse of technology or breaches of the Online Safety or Safeguarding Policies must be reported to the Headmistress via lowlevelconcerns@sarumhallschool.co.uk.

If the concern involves the Headmistress, it must be referred directly to the Chair of Governors in accordance with the school's safeguarding and whistleblowing procedures.

Appendix A – Online Safety Incident Flowchart



Th

Appendix B – Pupil Responsible Use Policy

Appendix C – Online Smart Rules