SARUM HALL

SCHOOL

ONLINE SAFETY POLICY

Date:	September 2024
Next Review Due:	September 2025
Reviewed by:	Chen Lee

INTRODUCTION

This Online Safety Policy outlines Sarum Hall School's commitment to safeguard members of our school community online in accordance with statutory guidance and best practice. It applies to all members of the school community (including staff, pupils, governors, volunteers, parents and carers, visitors) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Sarum Hall School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

RISKS AND HARMS

Online safety risks can be categorised under '4 Cs'. These are listed as follows:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: 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:** personal 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.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. Pupils or staff at risk can be reported to the Anti-Phishing Working Group (https://apwg.org/)

RESPONSIBILITIES

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

HEADTEACHER AND SENIOR LEADERS

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead (known as the Head of e-Learning), IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Head of e-Learning.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

GOVERNORS

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The Safeguarding Governor will:

- have meetings with the Designated Safeguarding Lead / Head of e-Learning;
- regularly receiving (collated and anonymised) reports of online safety incidents;
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended);
- ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by the Head of e-Learning, members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards;
- receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards.

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

DESIGNATED SAFETY LEAD (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role, supported by the Head of e-Learning;
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online;
- meet with the safeguarding governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out;
- attend relevant governing body meetings/groups;
- report regularly to headteacher/senior leadership team;
- be responsible for receiving reports of online safety incidents via CPOMS and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded;
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).

HEAD OF E-LEARNING (ONLINE SAFETY LEAD)

The Head of e-Learning will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL);
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments;
- have a leading role in establishing and reviewing the school online safety policies/documents;
- carry out annual filtering and monitoring checks;
- monitor and report on online safety incidents on CPOMS together with the DSL;
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond;
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents;
- provide (or identify sources of) training and advice for staff/governors/parents/carers/pupils;

- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particuarly by pupils) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

IT SUPPORT

Our technical staff, ITSupport (itsupport@sarumhallschool.co.uk) have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy;
- the school technical infrastructure is secure and is not open to misuse or malicious attack;
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body;
- there is clear, safe, and managed control of user access to networks and devices;
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Head of e-Learning for investigation and action;
- the filtering system, called SurfProtect by Exa Networks, is applied and updated on a regular basis;
- the monitoring system, Smoothwall by Qoria, is implemented and regularly reviewed.

TEACHING AND SUPPORT STAFF

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices;
- they understand that online safety is a core part of safeguarding;
- they have read, understood, and signed the Staff Responsible Use Policy;
- they immediately report any suspected misuse or problem to the Head of e-Learning and/or DSL for investigation/action, in line with the school safeguarding procedures;

- all digital communications with pupils and parents/carers are on a professional level and only carried out using official school systems;
- online safety issues are embedded in all aspects of the curriculum and other activities;
- ensure pupils understand and follow the Online Safety Policy and the pupils' ICT Responsible Use policy, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices;
- in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.;
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media;
- be aware the technology is a significant component in many safeguarding and wellbeing issues, such as sexting or being exposed to inappropriate content promoting extremism;
- be aware that child-on-child abuse can also occur online as well as in school.

PUPILS

- are responsible for using the school digital technology systems in accordance with the Pupils' ICT Responsible Use Policy and the Online Safety Policy;
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- should know what to do if they or someone they know feels vulnerable when using online technology;
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

PARENTS AND CARERS

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school's Online Safety Policy on the school website;
- providing them with a copy of the Pupils' ICT Responsible Use Policy in school planners;

- publish information about appropriate use of social media relating to posts concerning the school;
- seeking their permissions concerning digital images, cloud services etc;
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

REPORTING AND RESPONDING

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively;
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions;
- learning from the incident (or pattern of incidents) will be provided;
- the Designated Safeguarding Lead, Head of e-Learning and other responsible staff have appropriate skills and training to deal with online safety risks;
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP..

ONLINE SAFETY INCIDENTS FROM PUPILS

- Incidents relating to online safety and unacceptable use of technology by pupils will be reported on CPOMS with the Head of e-Learning alerted.
- If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen. Staff should reassure pupils that they have done nothing wrong. The incident should be reported to the Head of e-Learning and details of the website address and URL provided. The Head of e-Learning will liaise with the School's IT Support team to ensure that access to the site is blocked and the school's web filtering system reviewed to ensure it remains appropriate.
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
  - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported;
  - conduct the procedure using a designated device that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure;

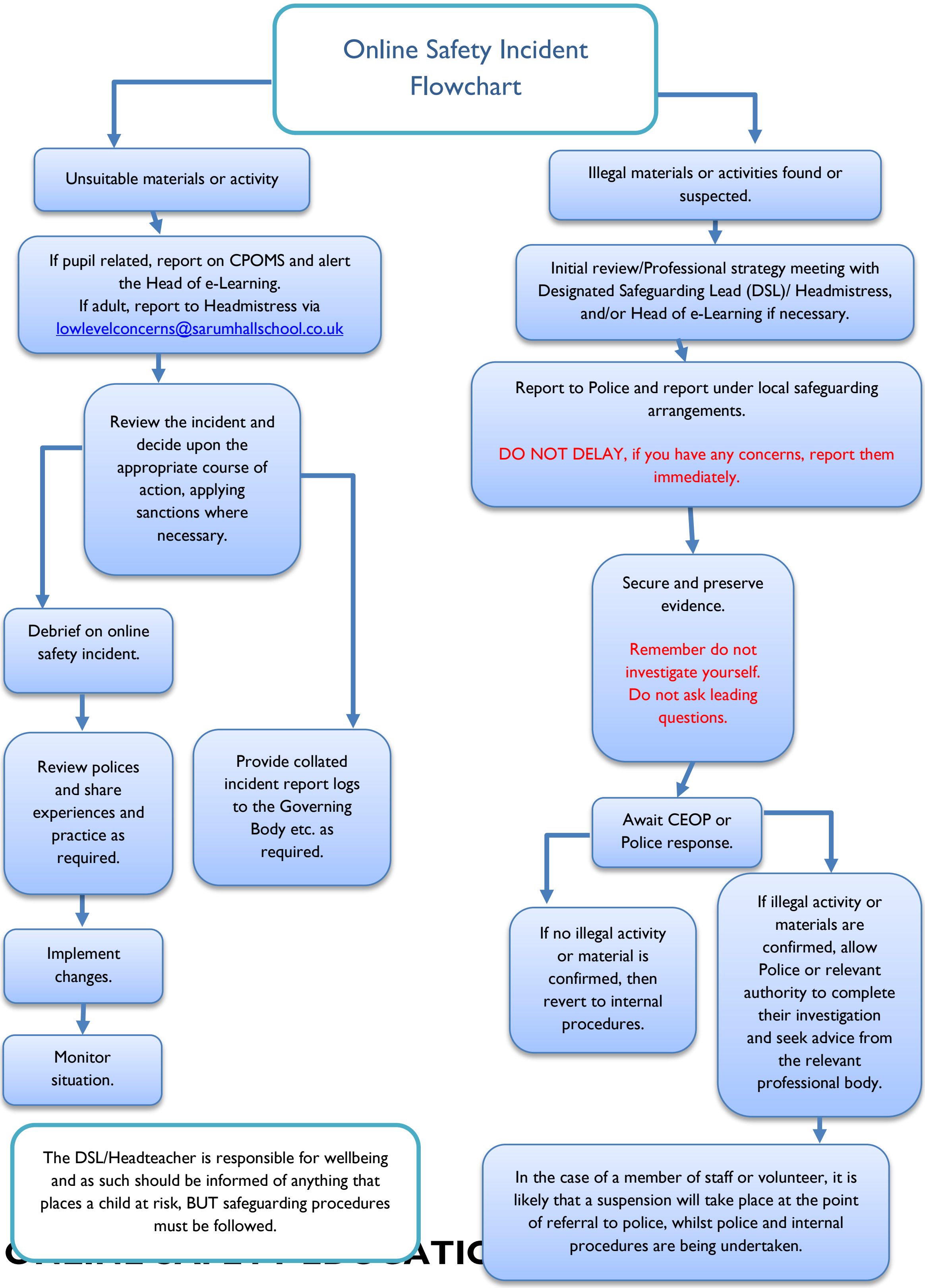
- ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection);
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation;
- once this has been completed and fully investigated the SLT, DSL and Head of e-Learning 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;
    - police involvement and/or action

SAFEGUARDING INCIDENTS

- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures, this may include:
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- Where concerns pertain to sexualised harms must be reported to the DSL immediately. If there is an incident/s where a member of staff knows an indecent image/video of a child (sometimes known as nude or semi-nude images) has been shared by pupils, they should never intentionally view the image, and must never copy, print, share, store or save such images. If a member of staff has already viewed the imagery by accident, this has to be reported to the DSL and advice sought. Staff must not ask the pupil to delete the imagery. In some cases, it may be more appropriate to confiscate any devices to preserve any evidence and hand them to the police for inspection. Please see section 18 of the Child Protection and Safeguarding Policy. More advice and guidance can be found in the government's Searching, Screening and Confiscation advice (for schools) and Sharing nudes and semi-nudes: how to respond to an incident.

STAFF INCIDENTS

- any concerns about staff misuse will be reported to the Headmistress via lowlevelconcerns@sarumhallschool.co.uk, unless the concern involves the Headmistress, in which case the complaint is referred to the Chair of Governors;



Online Safety Incident Flowchart

Unsuitable materials or activity

If pupil related, report on CPOMS and alert the Head of e-Learning.
If adult, report to Headmistress via lowlevelconcerns@sarumhallschool.co.uk

Review the incident and decide upon the appropriate course of action, applying sanctions where necessary.

Debrief on online safety incident.

Review polices and share experiences and practice as required.

Implement changes.

Monitor situation.

Provide collated incident report logs to the Governing Body etc. as required.

Illegal materials or activities found or suspected.

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Headmistress, and/or Head of e-Learning if necessary.

Report to Police 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 ask leading questions.

Await CEOP or 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.

The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

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

- A planned online safety curriculum is provided as part of computing and PSHE and is regularly revisited;
- Key online safety messages reinforced in annual online safety day/week, assemblies and form time/pastoral activities;
- Appointment of pupil Digital Leaders who are trained and then teach other pupils ways to stay safe online;
- Pupils are taught:
  - the potential risks of sharing too much personal information and talking to strangers online;
  - to identify signs and strategies to deal with cyberbullying (online bullying);
  - how their online reputation can be affected by what they publish and post online;
  - in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information especially with regards to online hoaxes;
  - how content and images online can affect their mental health, and understand how they can find advice and support to protect themselves;
  - about the dangers of online challenges and how to protect themselves from these;
  - to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making;
- Pupils are helped to understand the need for the Pupils' ICT Responsible Use Policy and encouraged to adopt safe and responsible use both within and outside school;
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices;
- In lessons where internet use is pre-planned, pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- Where pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit;

FILTERING

- The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

- Illegal content (e.g., child sexual abuse images) is filtered using SurfProtect by Exa Networks;
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective;
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that IT Support (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study;
- Filtering logs are regularly reviewed and the Designated Safeguarding Lead is informed by the Head of e-Learning to breaches of the filtering policy, which are then acted upon.

MONITORING

The school has monitoring systems in place to protect the school, systems and users:

- the school monitors all network use across all its devices and services using Smoothwall's monitoring system provided by Qoria. The system monitors in real-time risks on both staff and pupil devices. It captures user activity as it happens and these captures are then reviewed by Smoothwall moderators who will alert school of any urgent risks;
- monitoring reports are urgently picked up, acted on and outcomes are recorded by Head of e-Learning and the Designated Safeguarding Lead. All users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom);
- internet use is logged, regularly monitored and reviewed;
- filtering logs from the SurfProtect dashboard are regularly analysed and breaches are reported to senior leaders;
- *use of a third-party assisted monitoring service (Apple Classroom and Smoothwall).*

MOBILE TECHNOLOGIES

Please read the Staff Responsible Use Policy for Devices and E-mails.

USE OF DIGITAL AND VIDEO IMAGES

Please read the Taking, Storing and Using Images of Pupils Policy.

DATA PROTECTION

Please read the Data Protection Policy.