SARUM HALL

SCHOOL

E-SAFETY POLICY

Date:	September 2023
Next Review Due:	September 2024
Reviewed by:	Chen Lee

INTRODUCTION

This policy applies to all members of the school community (including pupils, staff, teaching, non-teaching and volunteers, including those in the Early Years Foundation Stage) who have access to and are users of school digital technology systems, both in and out of the school. Particular attention is paid to practices and procedures to help all members to adjust their behaviours in order to reduce risks. E-Safety is also known as online safety in this policy.

ROLE OF DESIGNATED SAFEGUARDING LEAD (DSL)

With the explosion in technology, we recognise that internet safety is a child protection and general safeguarding issue. This aspect is a role for our Designated Safeguarding Lead who is responsible for the safeguarding and welfare of pupils and our teaching staff. They work closely with the Head of e-Learning (also known as the Deputy Head (Academic and Innovation)) and the local authority safeguarding teams and other agencies in promoting a culture of responsible use of technology by all members of the community that is consistent with the ethos of Sarum Hall School. The DSL takes lead responsibility for understanding the filtering and monitoring systems and processes in place and will work alongside the Head of e-Learning to ensure that online safety practices are adhered to by all members of the school community and that a robust online safety education is delivered to pupils. The DSL and Head of e-Learning will work together to track and monitor any issues surrounding online safety.

ROLE OF HEADMISTRESS AND SENIOR LEADERSHIP TEAM

The Headmistress has a duty of care for ensuring the safety (including e-safety) of members of the school community, through the day to day responsibility for e-safety will be delegated to the Head of e-Learning.

The Headmistress/Senior Leadership Team are responsible for ensuring that the Head of e-Learning and other relevant staff receive suitable CPD training to enable them to carry out their e-safety roles and to train other colleagues, as relevant. They will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Head of e-Learning.

The Headmistress and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. It is the Headmistress's responsibility to handle allegations of misuse of the internet and technology.

ROLE OF HEAD OF E-LEARNING

The Head of e-Learning is responsible for developing, monitoring and reviewing the school's e-safety policy. They take day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies. They are responsible for ensuring that all pupils and staff adhere to the guidelines set out in the respective Responsible Use Policies (RUP) within school. E-safety lessons form part of the computing and PSHEE curriculum and these are evaluated annually by the Head of e-Learning and PSHEE Coordinator. They ensure that all staff are provided with regular training and advice so that they aware of the procedures that need to be followed in the event of an online safety incident taking place. Any minor internet-related incident is reported on CPOMS by staff and the Head of e-Learning is alerted. Any major safeguarding concern about a pupil's welfare can be reported on CPOMS as well but the DSL team will be alerted.

ROLE OF THE TECHNICAL STAFF (ITSUPPORT)

Our technical staff (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 the security of our hardware system and our data. A web content filtering system, called Surfprotect by Exa Networks, is in place to block sites thus preventing access to websites which could be unsuitable or disruptive for pupils to access. All websites are identified through an extensive category database which includes drugs, gambling, violence, intolerance and hate, criminal activity, spam, hacking, weapons and social networking sites. The school uses Smoothwall by Qoria to monitor 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.

ROLE OF SCHOOL STAFF AND EXTERNAL STAFF

All staff have a dual role concerning their own internet use and use of technology in any form, and providing guidance, support and supervision for pupils. Their role is to:

- Read, understood and signed the staff Responsible Use Policy for Mobile and Internet-Connected Devices for Staff;
- Adhere to the school's e-safety policies;
- Report any breaches of internet use, concerns about internet use or inappropriate use of technologies to the Head of e-Learning, DSL and/or to the Headmistress if a member of staff is involved;
- Be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use and use of technology, particularly in relation to their communications with pupils.

- 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.

ROLE OF PUPILS

Pupils will be responsible for using the school digital technology systems in accordance with the Pupil Responsible Use Policy. Through the curriculum, pupils will:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school.

ROLE OF PARENTS

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. We will take every opportunity to help parents understand these issues through *parents' evenings, bulletins, letters, website, social media and information about national/local online safety campaigns/literature.* Parents and carers will be encouraged to support the school in promoting good online safety practice and to comply with the following:

- To not use their mobile phones to make/receive calls or read/send messages when coming into the school and/or the Early Years setting;
- To not take photographs of children in the school and/or the Early Years setting unless for special events;
- To not to take photographs of other pupils on their own, without the prior agreement of that child's parents;
- To not photograph or record videos for other than their own personal use (e.g. with a view to selling videos of a school event);
- For specials events such as school performances or matches, photographs can be taken on the understanding that images that are not posted onto social media sites or otherwise shared. In this situation, parents are not covered by Data Protection Legislation.

RISKS AND HARMS

E-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/)

Where concerns pertain to sexualised harms are reported to staff, this must be reported to the DSL immediately. Staff should not view, copy or share the imagery of a child. 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. 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.

CYBERCRIME

Safeguarding guidance for schools has recently been updated to reflect the advances and emerge of wider e-safety harms and now makes specific reference to this issue (Keeping Children Safe in Education). This relates to criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber dependent crimes include:

- Unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test papers answers or change grades awarded
- Denial of Service (Dos or DDoS) attacked or 'booting'. These are attempts to make a computer, network, or website unavailable by overwhelming it with internet traffic from multiple sources; and;
- Making, supplying, or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets, and remote access trojans with the intent to commit further offence, including those above.

We recognise that children with a particular skill or interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns in this area Designated Safeguarding Leads should consider referring into the 'Cyber Choices' programme. This is a nationwide police initiative supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber dependent offences and divert them to a more positive use of their skills and interests.

Additional advice can be found at: https://www.nationalcrimeagency.gov.uk/cyber-choices

EDUCATION AND TRAINING

PUPILS

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. We want schools to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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 PSHEE and is regularly revisited;
- Key online safety messages reinforced in annual e-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;
- Pupils are taught to identify signs and strategies to deal with cyberbullying (online bullying);
- Pupils in KS2 are taught how their online reputation can be affected by what they publish and post online;
- Pupils are taught 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;
- Pupils are taught how content and images online can affect their mental health, and understand how they can find advice and support to protect themselves;

- Pupils are taught about the dangers of online challenges and how to protect themselves from these;
- Pupils are taught 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 Pupil Responsible Use Policies 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;
- 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.

PARENTS/CARERS

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website, parent portal;
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

STAFF/VOLUNTEERS

It is essential that all staff receive online safety training (including filtering and monitoring) and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.

- All new staff should receive online safety training/guidance as part of their induction programme, ensuring that they fully understand the school online safety policy and Responsible Use Policies.
- The Head of e-Learning will provide advice/guidance/training to individuals as required.

GOVERNORS

Governors will take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. The governors will ensure that all staff have had safeguarding training and online safety training which includes filtering and monitoring. They will discuss the DfE filtering and monitoring standards with the Head of e-Learning/ITSupport/service providers, and what more needs to be done to meet the standards.

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 which may include 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. More details can be found in the Responsible Use Policy for Mobile and Internet Connected Devices for Staff and the Child Protection and Safeguarding Policy.

USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users, including pupils, about these risks through and will implement policies to reduce the likelihood of the potential for harm. More information can be found in the Taking, Storing and Using Images of Pupils Policy.

DATA PROTECTION

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). More information can be found in the Data Protection and Privacy Policy.

RESPONDING TO INCIDENTS

Incidents relating to e-safety and unacceptable use of technology by pupils will be reported on CPOMS with the Head of e-Learning alerted. E-safety incidents involving safeguarding issues will be reported to the Designated Safeguarding Lead. Where the incident or complaint relates to a member of staff, the matter will be referred to the Headmistress for action via lowlevelconcerns@sarumhallschool.co.uk. Incidents involving the Headmistress will be reported to the Chair of the Board of Governors.

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. Pupils will be taught how to close or minimise the screen in computing sessions. Teachers 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. It is essential that teachers ensure that where they have an asked for filtering to be lifted for a particular lesson (e.g. sex education) that they notify the school's IT Support team so that filtering can be put back to minimise the risk of inappropriate sites being accessed by pupils or staff.

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. The member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy). Please see section 18 of the Child Protection and Safeguarding Policy.

If a member of staff is aware of the misuse of technology by a colleague, they should report this to the Headmistress immediately via lowlevelconcerns@sarumhallschool.co.uk. IT Support will be informed accordingly so that the computer or laptop is taken out of use and securely stored in order to preserve any evidence. A note of any action taken will be recorded. Once the facts are established, the Headmistress should take any necessary disciplinary action against the staff member and report the matter to the governors and the police, where appropriate.

MISUSE: STATEMENT OF POLICY

We will not tolerate any illegal material, and will always report illegal activity to the police. If we discover that a child or young person is at risk as a consequence of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). We will impose a range of sanctions on any member of the community who misuses technology to bully, harass or abuse in line with our Prevent Bullying policy. Notifications will be made to the Local Authority and Ofsted in the event of an allegation of serious harm or abuse by any person working in the school or the Early Years setting.