Sarum Hall School

e-SAFETY POLICY ON USE OF INFORMATION COMMUNICATION TECHNOLOGY

Date: Oct -17
Review: Date: Oct -18

This policy applies to all members of the school community: pupils, staff, teaching, non-teaching and volunteers, including those in the Early Years Foundation Stage.
Particular attention is paid to practices and procedures to help all members to adjust their behaviours in order to reduce risks, including the safe use of information and communication technologies.

TECHNOLOGY IN THE CURRICULUM

Technology has transformed the entire process of teaching and learning at Sarum Hall School. It is a crucial component of every academic subject, and is also taught as a subject in its own right. Our classrooms are equipped with interactive whiteboards and computers. We have a computer suite in the school and pupils may use the machines for their private study with adult supervision. We also have Chromebooks and iPads for use by all teachers in their lessons.

All of our girls are taught how to research on the internet and to evaluate sources. They are educated in the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution.

THE ROLE OF TECHNOLOGY IN OUR LIVES

Technology plays an important part in the lives of all members of our community. Sophisticated games consoles (like PS4 and Nintendo Switch), together with mobile phones provide unlimited access to the internet, to social media services where you upload media content (like Facebook, Instagram, YouTube and Musical.ly), to peer-to-peer communication services (like Snapchat, Facetime and Whatsapp). Girls are made aware that all social media accounts have a minimum age restriction of at least 13.

This communication revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at Sarum Hall to teach pupils and staff how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks linked to the potential Content, Contact and Conduct within websites, including identity theft, bullying, harassment, grooming, radicalisation stalking and abuse. They also learn how to avoid the risk of exposing themselves to subsequent embarrassment.

THE ROLE OF OUR TECHNICAL STAFF

With the explosion in technology, we recognise that blocking and barring sites is no longer adequate. We need to teach all of our pupils to understand why they need to behave

responsibly if they are to protect themselves. This aspect is a role for our Designated Senior Person who is responsible for the safeguarding and welfare of girls (Mrs Smith) and our teaching staff.

Our technical staff has 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, our data and for training our teaching and administrative staff in the use of technology. They monitor the use of the internet and emails and will report inappropriate usage. A web content filtering system is in place to monitor and 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.

Future Digital Safeguarding Software is installed on the school computers which alerts the staff if the Responsible Use policy has been breached by any person using the network, or of potential child protection issues. This protects pupils and other users of the network from cyberbullying, online grooming, explicit images and harmful sites such as those promoting suicide, anorexia and radicalisation, among other threats (Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism.) The software takes a screen capture anytime certain words or phrases appear on the screen. The captures are reviewed and graded every day by the E-safety Officer.

ROLE OF DESIGNATED SENIOR PERSON (DSP)

We recognise that internet safety is a child protection and general safeguarding issue. Mrs Smith is our DSP and has been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. She works closely with the Local Safeguarding Children's Board (LSCB) 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. All of the staff with pastoral responsibilities have also received training in e-safety issues. The DSP will ensure that all year groups in the school are educated in the risks and the reasons why they need to behave responsibly online. There is a dedicated scheme of work that has been produced for Reception – Year 6 on age-appropriate e-safety issues. It is Mrs Smith's responsibility to handle allegations of misuse of the internet and technology.

ROLE OF E-SAFETY OFFICER

The E-safety Officer is responsible for developing, monitoring and reviewing the school's e-safety policy. The Officer should hold accredited training, for example CEOP ambassador training. They are responsible for ensuring that all pupils and staff have read and signed the Responsible Use Policy (RUP). The E-safety Officer works closely with the IT manager to ensure that they are up to date with e-safety issues and to advise of any new trends, incidents and arising problems to the head teacher. A dedicated scheme of work has been produced which will be evaluated annually by the E-safety Officer. A log of internet-related incidents will be kept by the Officer and will work closely with Mrs Smith when dealing with allegations of misuse of the internet and technology by members of the community. The

Future Digital Safeguarding Software log of screen captures are reviewed daily by the Officer.

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 adhere to the school's e-safety and Responsible Use policies and to communicate them to pupils. They report any breaches of internet use, concerns about internet use or inappropriate use of technologies to the E-safety Officer or to the Headmistress.

School staff needs to 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.

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations. More detail on roles and responsibilities are outlined in the Responsible Use of the Internet & Mobile Devices for Staff and Volunteers Policy.

Personal devices (e.g. mobiles, tablets and laptops) within school and/or the Early Years Setting

- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode and not used during teaching periods unless in emergency circumstances;
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and should only use school provided equipment for this purpose;
- Staff must not copy and store images or recordings of pupils on their personal devices;
- Staff use of mobile phones during the school day will be limited to the breaks and after school, only in designated areas such as the staff room or in a private room away from children and not in open areas;

Contacting parents

- Staff are **not** permitted to use their own mobile phones or devices for contacting pupils, young people or those connected with the family of the student via instant messaging or social networking sites;
- Staff will be issued with a school phone where contact with pupils, parents or carers is required, for example a mobile on school trips or staff based landline in departments or school offices. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off- site activities, or for contacting parents, they should use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes;

Data and Network Protection

- If you leave your computer for any period of time, you should lock your screen or log off;
- Personal or school data must be password protected and encrypted if uploaded onto a cloud service or taken off the school premises. For files created on MS Office 2016, click "File" and then "Info" to see Microsoft's document options. Click "Protect Document," and then select "Encrypt with Password" to open the Encrypt Document dialog box;
- Under no circumstances should you view, download or upload material which is likely to be unsuitable for children;
- If using the Internet with a class, ensure that the girls have followed the correct procedures throughout the session.

Online Apps and websites

- Staff should always use school equipment and only store images on the school computer system, with all other copies of the images erased. Staff must never use a personal device to take a photograph, record pupils, or play music.
- Do not contact the parents or children via telephone, email, or social media including Facebook, Instagram, twitter, including fliers and/or information about competitions, holiday clubs, etc.
- Staff should ensure that any materials published on their own social networking sites or any website in relation to themselves are neither inappropriate nor illegal, with due consideration shown towards the reputation of their profession.
- Staff should be particularly careful regarding any comments to do with the school or specific pupils that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.

ROLE OF PARENTS

- Parents and carers are asked to not use their mobile phones to make or receive calls, read or send messages, when they are coming into the school and/or the Early Years setting;
- Parents are generally prohibited from taking any photographs of children in the school and/or the Early Years setting, but for special events such as school performances or matches, may do so on the understanding that the **images are not posted onto social media sites or otherwise shared**. In this situation, parents are not covered by the Data Protection Act 1998. When an event is held indoors, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others.
- Parents are not permitted to take photographs or to make a video recording for anything other than their own personal use (e.g. with a view to selling videos of a school event). We ask parents not to take photographs of other pupils on their own, without the prior agreement of that child's parents. Parents, staff or visitors who suspect anyone of taking images of children without consent must report the incident to the Headmaster immediately.

MISUSE: STATEMENT OF POLICY

We will not tolerate any illegal material, and will always report illegal activity to the police and/or the Local Child Safeguarding Board (LCSB). 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 anti-bullying policy. Notifications will be made to Ofsted in the event of an allegation of serious harm or abuse by any person working in the school or the Early Years setting.

COMMON RISKS LIKELY TO ENCOUNTER ONLINE

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse;
- lifestyle websites, for example pro-anorexia/self- harm/suicide sites;
- hate sites;
- content validation: how to check authenticity and accuracy of online content;

Contact

- grooming;
- cyber-bullying in all forms;
- identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords;

Conduct

- privacy issues, including disclosure of personal information;
- digital footprint and online reputation;
- health and well-being (amount of time spent online (internet or gaming));
- sexting (sending and receiving of personally intimate images);
- copyright (little care or consideration for intellectual property and ownership (for example music and film)).

RESPONDING TO INCIDENTS

All incidents and complaints relating to e-safety and unacceptable use of technology will be reported to the E-safety Officer who will record it on the e-Safety Incident Report Form.

Where the incident or complaint relates to a member of staff, the matter will be referred to the Headmistress for action. Incidents involving the Headmistress will be reported to the chair of the board of governors. E-safety incidents involving safeguarding issues will be reported to the Designated Senior Person.

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 also be taught to close or minimise the screen. Teachers should reassure pupils that they have done nothing wrong. The incident should be reported to the E-safety Officer and details of the website address and URL provided. The E-safety

Officer 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 team so that filtering can be put back to minimise the risk of inappropriate sites being accessed by pupils or staff.

If a member of staff is aware of the misuse of technology by a colleague, they should report this to the Headmistress or the E-safety Officer immediately. The network manager should be informed 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 should be recorded on the e-safety incident report form. Once the facts are established, the head teacher should take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate.

INVOLVEMENT WITH PARENTS AND GUARDIANS

We seek to work closely with parents and guardians in promoting a culture of e-safety. We will always contact parents if we have any worries about their daughter's behaviour in this area, and we hope that they will feel able to share any worries with us. We recognise that not all parents and guardians may feel equipped to protect their daughter when they use electronic equipment at home. We therefore arrange occasional discussion evenings for parents when an outside specialist advises about the potential hazards of this exploding technology, and the practical steps that parents can take to minimise the potential dangers to their daughters without curbing their natural enthusiasm and curiosity. Our website and Intranet contains links to websites which parents and guardians can refer to regarding the safe use of technology. Copies of the pupils' Responsible Use policies are available on the school's Intranet.

GUIDANCE FOR THE SAFE USE OF TECHNOLOGIES

E-safety is a whole school responsibility, and at Sarum Hall School, the staff and pupils have adopted the following guidelines for the safe use of technologies

Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying, because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. Our school's anti-bullying policy describes our preventative measures and the procedures that will be followed when we discover cases of bullying.
- Proper supervision of pupils plays an important part in creating a safe IT environment at school; but everyone needs to learn how to stay safe outside the school.
- We value all members of our community equally. It is part of the ethos of Sarum Hall School to promote considerate behaviour, and to value diversity.
- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.

Treating Other Users with Respect

- We expect all members of the school community to treat each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. They should always follow the school's Golden Rules and adhere to the Code of Conduct.
- We expect a degree of formality in communications between staff and pupils, and would not normally expect them to communicate with each other by text or mobile phones. Our policy on Educational Visits explains the circumstances when communication by mobile phone may be appropriate.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. Our Anti-bullying policy is set out on our website. The school is strongly committed to promoting opportunities for all, regardless of race, gender, gender orientation or physical disability.
- All members of the community are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issue to a member of staff.
- The use of cameras is not allowed in washing and changing areas.
- The cameras, visualizer camera, webcam and the camera function on the school iPads and Chromebooks may be used by pupils and teachers for educational purposes under teachers' supervision.
- Mobile phones belonging to pupils are not permitted and are handed into the office for safekeeping. The school does not accept responsibility for such devices.
- Staff use of the internet and e-mail for personal use on the school computers or on personal devices during working hours should be reasonable and limited to lunchtimes, playtimes or after school when children are not present.

Keeping the School Network Safe

- Certain sites are blocked by our filtering system and our IT Support monitors pupils' use of the network.
- The IT Support monitors e-mail traffic and blocks SPAM and certain attachments.
- We issue some pupils with their own personal school email address. Access is via personal LOGIN, which is password protected. We give guidance on the reasons for always logging off and for keeping all passwords securely.
- Access to sites such as "hotmail" and Facebook are not allowed on the school's network.
- Teachers' access to some social networking sites will be allowed on the school network for educational purposes. If these networking sites have educational purposes for the pupils, teachers will ensure that the website is age appropriate and does not have age restrictions which would apply to our pupils.
- We have strong anti-virus protection on our network, which is operated by IT Support.
- Any member of staff or pupil, who wishes to connect a removable device to the school's network, is asked to arrange in advance with the IT Support to check it for viruses.
- Staff will not download any software from the Internet that can compromise the network, or are not adequately licensed. Any software requests need to be

confirmed with the IT support team and the team will install if they are appropriate for the network.

Promoting Safe Use of Technology

Responsible use policies

All staff and pupils sign a Responsible Use Policy that sets out their rights and responsibilities and incorporates the school e-safety rules regarding their use of technology. The pupils' RUPs are also signed by their parents.

E-safety curriculum

The safe use of technology is taught to pupils of all ages through Computing and PSHEE lessons, presentations, assemblies and discussion in the meetings of the School Council. Particular attention is paid to school practices to help children to adjust their behaviours in order to reduce risks and build resilience, including to radicalisation, with particular attention to the safe use of electronic equipment and the internet. These practices are age appropriate and delivered through a planned component of the curriculum. Children should understand the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults. The curriculum for all pupils from Rec to Year 6 can be found here: E-safety curriculum and resources.

Girls are encouraged to make use of the online resources that are available from sites such as:

- Childnet International (www.childnet-int.org)
- Digizen (www.digizen.org.uk)
- Think you Know www.thinkuknow.co.uk
- Kidsmart www.kidsmart.org.uk
- Cyber Mentors (www.cybermentors.org.uk)
- Cyberbullying (www.cyberbullying.org)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)

The sites cover the different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment, identity theft, copyright and plagiarism. Guidance covers topics such as saving yourself from future embarrassment, explaining that any blog or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or internet archive and cause embarrassment years later. We offer guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.

Pupils in Year 6 are provided with a personal login password and a password reminder is stored by the Head of Computing teacher.

We give guidance on how to keep safe at home.

Pupils' Considerate Use of Electronic Equipment

- Mobile phones and other personal electronic devices should be switched off and stored in the office securely during the school day.
- Staff may confiscate personal equipment that is being used during the school day.

We expect all pupils to adhere to this guidance for the safe use of the internet. Staff, Parents and girls are asked to read and sign the 'Responsible Use of the Internet and Mobile Devices' forms which are retained by the school office.

We may impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devices which adheres to the sanctions outlined in the school's behaviour policy.

Linked guidance, policies and procedures:

Keeping Children Safe in Education (KCSIE) statutory guidance

Working_together_to_safeguard_children.pdf

Criminal Law
The Department for Education (DfE)
The Independent Schools Inspectorate (ISI)
School Policies including EYFS
Sarum Hall Mission Statement
Public Health Agencies
Code of Conduct.