E-SAFETY POLICY ON USE OF INFORMATION COMMUNICATION TECHNOLOGY

Date: May-22
Review: Date: May-23

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.

ROLES AND RESPONSIBILITIES

ROLE OF DESIGNATED SAFEGUARDING AND PREVENT 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 and Prevent Lead (the Headmistress) who is responsible for the safeguarding and welfare of girls and our teaching staff. She 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 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. All of the staff will receive regular training in e-safety issues. The DSL will ensure that all year groups in the school are educated in the risks and the reasons why they need to behave responsibly online. 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. He takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies. He is responsible for ensuring that all pupils and staff adhere to the guidelines set out in the respective Responsible Use Policies (RUP) within school and the Remote Learning Agreement outside of school. A scheme of work has been produced which will be evaluated annually by the Head of e-Learning. He ensures that all staff are provided with 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. A log of internet-related incidents will be kept by the Officer and he reports regularly to Senior Leadership Team.

ROLE OF OUR TECHNICAL STAFF

Our technical staff 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, 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.

Smoothwall 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 or are typed. The captures are reviewed regularly by the Smoothwall team.

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 and the Remote Working Mobile Device Policy;
- 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 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 peer on peer 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 and the Remote Learning Agreement. 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, newsletters, 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.

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;
- 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;
- 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 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, Learning Platform;*
- *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 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 as part of their induction programme, ensuring that they fully understand the school online safety policy and Responsible Use Policies and Remote Learning Agreement.
- 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.

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 the school's learning platform and other 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 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.

REMOTE WORKING

On occasions, staff may need to use mobile devices remotely for work purposes (whether owned personally or by the school). The Remote Working Mobile Device Policy provides information to ensure that staff are aware of the risks associated with using mobile devices remotely in terms of the security of the School's IT resources and systems, and the steps that must be taken to comply with the School's legal obligations and protect personal data and confidential and proprietary information of the School.

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

All incidents and complaints relating to e-safety and unacceptable use of technology will be recorded on e-Safety Incident Report Form and then reported to the Head of e-Learning who will record it on the e-Safety Incident Log. 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 Safeguarding and Prevent Lead.

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.

Please see Annex C of the KCSIE Child Protection and Code of Conduct Policy if there is an incident/s where nudes and semi-nudes have been shared by pupils.

If a member of staff is aware of the misuse of technology by a colleague, they should report this to the Headmistress immediately. IT Support 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.

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 Prevent 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.

LINKED GUIDANCE, POLICIES AND PROCEDURES:
Keeping Children Safe in Education (KCSIE) statutory guidance 2021
Working together to safeguard children
Teaching Online Safety in Schools
Education for a Connected World Framework

Relevant school policies:
Keeping Children Safe in Education 2021, Child Protection Policy and Code of Conduct.