



E-SAFETY POLICY FOR STUDENTS AND PARENTS

This policy should be read in conjunction with the ICT Policy (staff) and Student Behaviour and Sanctions Policy.

SCHOOL AIMS

South Wilts is a progressive grammar school which aims to maintain high academic standards and cultural achievement within a caring environment. We seek to encourage responsibility and personal fulfilment so that students attain their maximum potential. The School is dynamic and works with the community to prepare its students for life-long learning and adult independence.

South Wilts Grammar School values and respects all students equally and aims to provide equality of opportunity wherever possible.

South Wilts is committed to safeguarding and promoting the welfare of children. The school fulfils its responsibilities as laid out in the following key documents: Working Together to Safeguard Children, Keeping Children Safe in Education and the procedures of the Safeguarding Vulnerable People Partnership.

Safeguarding links/ risks associated with this policy: This policy should be read in conjunction with the Safeguarding and Child Protection Policy, the Staff Code of Conduct and the WSCB Social networking procedure.

RESPONSIBILITY

Internet safety depends on staff, trustees, parents and the students themselves taking responsibility for the use of internet and other communication technologies such as mobile phones. The balance between educating students to take a responsible approach and the use of regulation and technical solutions will be judged carefully. The school and Smoothwall limit internet access, in line with this E-Safety Policy.

There are no straightforward or totally effective solutions and staff, parents and the students themselves must remain vigilant.

- All users are protected from inappropriate material, bullying and harassment
- User have access to resources to support learning and teaching
- Users are given clear boundaries on responsible and professional use
- Access to the internet may be unsupervised e.g. at lunchtimes

AUTHORISATION OF USE

Internet access for students should be seen as an entitlement on the basis of educational need and an essential resource for staff. Parental permission will be sought at the start of each Key Stage.

- The school will keep a record of all students who are granted internet access. The record will be kept up-to-date
- Students must agree to abide by the Responsible Internet Use Statement that is signed in conjunction with their parents. They must also agree to the Responsible Use Policy at logon and at appropriate intervals in order to use the school network
- Students must apply for Internet access individually by agreeing to abide by the Responsible Use Policy statement that is signed in conjunction with their parents
- Parents will be informed that students will be provided with supervised Internet access

FILTERING

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the student's age and experience. Internet access must be appropriate for all members of the school community from youngest student to staff.

- The school will work in partnership with parents, Wiltshire Council, DfE and Smoothwall to ensure systems to protect students are reviewed and improved
- The school receives Internet Service Provision (ISP) from Broadband4 and use Smoothwall to proactively monitors Internet usage for attempts to access illegal (child abuse and incitement for racial hatred) content and will notify the local police and Wiltshire Council in these instances
- If staff or students discover unsuitable sites, the URL (web address) and content must be reported to the Designated Safeguarding Lead (DSL)
- Website logs will be sampled and monitored where necessary
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

RISK ASSESSMENT

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation.

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access
- Methods to identify, assess and minimise risks will be reviewed regularly
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

EVALUATING CONTENT

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular, it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read.

Ideally inappropriate material would not be visible to students using the web but this is not easy to achieve and cannot be guaranteed. Students should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- The DSL / SLT as appropriate will be responsible for permitting and denying additional websites as requested
- Students will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum
- The school will ensure that the use of Internet derived materials by staff and by students complies with copyright law

SWGS WEBSITE CONTENT

Publication of any information online should always be considered from a personal and school security viewpoint. Sensitive information may be better published in the school handbook or on a secure online area which requires authentication. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or students' personal information will not be published
- Website photographs that include students will be selected carefully
- For year 7 students, written permission from parents or carers will be obtained before photographs of students are published on the school website. For year 8 and above, students are asked to give permission. Photographs will be selected carefully and will not enable individual students to be named
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright

E-MAIL

E-mail is an essential means of communication for both staff and students. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

- The only e-mail account that may be accessed on the school systems is the allocated school e-mail account
- Students must immediately report any offensive e-mails

- Students must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone through an e-mail contact
- Students cannot send multiple copies of e-mails to more than 5 recipients
- Staff will use official school provided email accounts for all communication with students
- Students should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly
- E-mail sent to an external organisation should be written carefully in the same way as a letter written on school headed paper

SOCIAL NETWORKING AND COMMUNICATION

On-line communications, social networking and social media services are filtered in school by the SWGfL but are likely to be accessible from home.

All staff are made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They are made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Students are encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Schools have a key role to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private.

- Students will be taught about how to keep personal information safe when using online services. Each Key Stage will have specific ICT lessons dedicated to e-safety. This will be further emphasised in main assemblies
- The school will conduct student surveys about home use of ICT. It will gauge the range of activities which students undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.
- The use of online chat is not permitted in school
- The use of inappropriate text, images and videos about other students or staff is unacceptable and will always be fully investigated once discovered
- Users will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Users must not reveal personal details of themselves or others in online communication, or arrange to meet anyone
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the DSL before using Social Media tools in the classroom
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible

- Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Student will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private
- No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory
- Parents wishing to photograph or video at an event should be made aware of the school's expectation. We will ask parents to ensure that all photos are of their son or daughter. Photos that contain images of other students must not be uploaded to social media sites.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' staff must not engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites

MOBILE DEVICES

Mobile devices refer to any device that provides access to the internet or internal network for example tablets, e-readers, mobile phones, laptops, ipads and digital cameras.

- Students are allowed to bring mobile devices to school but they must be set to silence and out of sight at all times, unless specifically directed by a member of staff
- The sending of abusive or inappropriate messages is forbidden by any member of the school community
- We will advise parents to discuss the issues concerning students connecting to the internet using their mobile devices using mobile data as this cannot be monitored by the school
- Mobile devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items
- School staff, authorised by the head teacher may search students or their possessions and confiscate any mobile device if they believe it is being used to contravene the school policy. If it is suspected that the material on the mobile device relates to a criminal offence, the device will be handed over to the police for further investigation
- Mobile devices may be used during lessons or formal school time as part of an approved and directed curriculum-based activity with consent from a member of staff
- Where staff need to contact children, young people and their families within or outside of the setting in a professional capacity, they should do so via an approved school account (e.g. e-mail, phone, social media) In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to the DSL
- For the safeguarding of all involved, users are encouraged to connect mobile devices through the school wireless provision and service that allows the ability to

filter any device that uses the school Internet connection, without having to configure the user's device

- The school will take steps to monitor responsible use in accordance with the Responsible Use Policy

Teaching and Learning

Why is Internet use important?

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires students to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed, ICT is now seen as an essential life-skill.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and students
- The purpose of Internet use in school is to raise educational standards, to promote student achievement, well-being and to support the professional work of staff and to enhance the school's management information and business administration systems
- Internet access is an entitlement for students who show a responsible and mature approach to its use
- The Internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience
- Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security

How will Internet use enhance learning?

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between students worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for students and staff;
- Professional development for staff through access to national developments,
- Educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.

Video Conferencing

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education.

- Staff will refer to the internet consent agreements prior to children taking part in videoconferences
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer
- Students must ask permission from a teacher before making or answering a videoconference call
- Videoconferencing will be supervised appropriately for the students' age and ability

Cyber Bullying

Cyber bullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007.

For most, using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff and parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyber bullying (along with other forms of bullying) of or by any members of the school community will not be tolerated.

- Clear procedures are set out to investigate incidents or allegations of cyber bullying
- Clear procedures in place to support anyone in the school community affected by cyber bullying
- All incidents of cyber bullying reported to the school will be recorded
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary
- Students, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's e-Safety ethos

Data Protection

The quantity and variety of data held on students, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The General Data Protection Regulations (GDPR) / Data Protection Act 2018 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected. For advice and guidance relating to a contravention of the Act, contact the Data Protection Officer (I – West, Audit West, Bath and North East Somerset Council, Guildhall, High Street, Bath, BA1 5AW or via email at i-west@bathnes.gov.uk~)

Many students are very familiar with Internet use and the culture that surrounds it. As part of the school's e-safety teaching and awareness-raising it is important to discuss the key features with students as appropriate for their age. Students may need to be reminded of the school rules at the point of Internet use.

- Rules for internet access will be posted in all rooms where computers are used and will be shown as a Responsible Use Policy on all computer monitors after students log-on
- Students will be informed that internet use is monitored
- Online safety teaching will be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst students
- Online safety teaching will be included in the PSHE, Citizenship and/or ICT scheme of work, covering both safe school and home use
- Online Safety rules or copies of the student Responsible Use Policy will be on display in all rooms with Internet access
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas

SANCTIONS

- The school's Student Behaviour and Sanction Policy applies to responsible ICT use
- Responsibility for handling incidents will be delegated to a senior member of staff
- Sanctions available include:
 - Interviews with senior staff
 - Informing parents or carers
 - Removal of internet or computer access for a period
 - Possible involvement of the police
 - Any complaint about staff misuse must be referred to the Headteacher

Policy in Practice – Staff

It is important that all staff feel confident to use new technologies in teaching and the School e-Safety Policy will only be effective if all staff subscribe to its values and methods. Staff are given opportunities to discuss the issues and develop appropriate teaching strategies. Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff

Policy in Practice – Parents

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk. We will refer parents to websites where they can obtain further advice and guidance. Links will be included on the school website for this and regular reminders of this in the school newsletter.

- Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school website

- A partnership approach with parents will be encouraged. This could include offering parent evenings, demonstrations, practical sessions and suggestions for safe Internet use at home
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home
- Internet issues will be handled sensitively to inform parents without undue alarm
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents

Handling of complaints

Parents and teachers must know how and where to report incidents. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All record of the incident will be kept, e.g. e-mails, saved or printed, text messages saved etc. Complaints of a child protection nature will be dealt with in accordance with the LA Child Protection procedures.

- Responsibility for handling incidents will be delegated to a senior member of staff
- Any complaint about staff misuse must be referred to the headteacher
- Students and parents will be informed of the complaints procedure
- Parents and students will need to work in partnership with staff to resolve issues
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies

School-sanctioned use of social media

There are many legitimate uses of social media within the curriculum and to support student learning. There are also many possibilities for using social media to enhance and develop students' learning.

When using social media for educational purposes, the following practices must be observed:

- The URL and identity of the site should be notified to the appropriate Head of Department or member of the SLT before access is permitted for students
- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and ideally should be linked to an official school email account
- Care must be taken that any links to external sites from the account are appropriate and safe
- Any inappropriate comments on, or abuse of, school-sanctioned social media should immediately be removed and reported to a member of SLT
- All social media accounts created for educational purposes should include a link in the About or Info page to the ICT Acceptable Use Policy on the school website. This will indicate that the account is officially sanctioned by South Wilts Grammar School

Monitoring of Internet Use

South Wilts monitors usage of its internet, online content, online services and email services without prior notification or authorisation from users.

Users of South Wilts email and internet services should have no expectation of privacy in anything they create, store, send or receive using the school's ICT system.

Breaches of this Policy

Any breach of this policy that leads to a breach of confidentiality, defamation or damage to the reputation of South Wilts or any illegal acts or acts that render South Wilts liable to third parties may result in legal action, disciplinary action or sanctions in line with the published school policies

Reviewed by	Date of Review / approval	Review cycle	Next Review Date	Statutory / Non statutory	Website
Resources	Autumn 2024	Annually	Autumn 2025	Non-Statutory	Yes