



SOUTH WILTS GRAMMAR SCHOOL FOR GIRLS (ACADEMY)

SCHOOL AIMS

South Wilts is a progressive grammar school for girls 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.

E-SAFETY POLICY

RESPONSIBILITY

Internet safety depends on staff, governors, 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 the SWGfL 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 staff and 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 the SWGfL to ensure systems to protect students are reviewed and improved

- The school receives Internet Service Provision (ISP) from South West Grid for Learning (SWGfL) and have a service which 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
- A log of all staff with privileged access to the Internet will be kept and regularly reviewed
- If staff or students discover unsuitable sites, the URL (web address) and content must be reported to the Designated Senior person (DSP)
- 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
- The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored

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. A whole curriculum approach may be required.

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 DSP 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
- Students will use age-appropriate tools to research Internet content
- 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

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
- Written permission from parents or carers will be obtained before photographs of students are published on the school website. Photographs will be selected carefully and will not enable individual students to be named
- Students' full names will not be used anywhere on the website, particularly in association with photographs
- 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 school business
- 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 and copied to the pinks, 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, other than as part of its online learning environment when directed by a member of staff
- 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 DSP before using Social Media tools in the classroom
- Staff official blogs or wikis should be password protected and run with approval from the DSP
- 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 and should seek advice from the DSP
- 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
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Responsible Use Policy
- 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, ipads and digital cameras.

- Students are allowed to bring mobile devices to school but they must set to silence and out of sight except at break and lunchtimes, unless specifically directed by a member of staff
- The sending of abusive or inappropriate messages is forbidden by any member of the school community
- Parents should advise the appropriate use of mobile devices for access to the internet 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 DSP
- Staff will be issued with school equipment for taking photos or video of students linked to an educational intention. In exceptional circumstances staff may need to use personal devices for such purpose and when doing so, must ensure they comply with the schools Responsible Use Agreement
- 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.

Virtual Learning Environment (VLE)

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, students and parents, as well as support for management and administration.

- SLT and staff will regularly monitor the usage of the VLE by students and staff in all areas, in particular message and communication tools and publishing facilities
- Students/staff will be advised about acceptable conduct and use when using the VLE
- Only members of the current student, parent/carers and staff community will have access to the VLE
- All users will be mindful of copyright issues and will only upload appropriate content onto the VLE
- When staff, students etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment

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 must 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

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed

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 Data Protection Act 1998 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 www.wiltshire.gov Wiltshire council guidance for schools here:

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

Policy in Practice – Students

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 Behaviour 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 should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside of the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their senior leader to avoid any possible misunderstanding.

- All staff must refer to the relevant detail in the Staff Handbook and adhere to the school's E-safety Policy
- Staff should be aware that internet traffic is monitored and reported by the school and the SWGfL and can be traced to the individual user. Discretion and professional conduct is essential

- The monitoring of staff internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management
- The Online Safety Policy will be provided to and discussed with all members of staff and Responsible User Policy signed for compliance
- 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
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities

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. School will refer parents to websites referred to in the references section of this document.

- 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

Appendix

Social Media Policy

1. Rationale

1.1 The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation. For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

1.2 The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice. They apply to all members of staff at the school.

The purpose of the policy is to:

- Safeguard all children
- Protect the school from legal risks
- Ensure that the reputation of the school, its staff and governors is protected
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the school

2. Definitions and Scope

2.1 Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications, and online gaming environments. Examples include Twitter, Facebook, Windows Live Messenger, YouTube, Flickr, Xbox Live, Blogger, Tumblr, Last.fm, and comment streams on public websites such as newspaper sites.

2.2 Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

- Users should be conscious at all times of the need to keep their personal and professional/school lives separate. They should not put themselves in a position where there is a conflict between the school and their personal interests
- Users should not engage in activities involving social media which might bring SWGS into disrepute
- Users should not represent their personal views as those of SWGS on any social medium
- Users should not discuss personal information about pupils, SWGS and the wider community they interact with on any social media
- Users should not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations or SWGS

2.3 All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the school's Equalities, Child Protection and ICT Acceptable Use Policies.

2.4 Within this policy there is a distinction between use of school-sanctioned social media for professional educational purposes, and personal use of social media.

3. Use of Social Media in practice

3.1 Personal use of social media:

- Members of the wider school community should not identify themselves as members of South Wilts in their personal web-space, unless specifically linked to an approved job role within the school community where it serves a purpose to professionally market the school. This is to prevent information being linked with the school and to safeguard the privacy of staff members, pupils and parents and the wider school community
- School staff must not invite, accept or engage in communications with children from the school community in any personal social media whilst in employment at South Wilts Grammar School
- Where friendships exist between school staff and parents before they become parents, i.e. before their daughters attend SWGS, we would not expect these friendships to change, but staff would need to be mindful of comments that they make in relation to the school. It might also be prudent to review photos where they have been tagged with a member of staff's name
- Staff should not accept any current student of any age or any ex-student of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account
- Any communication received from children on any personal social media sites must be reported to the designated person for Child Protection (Deputy Headteacher, Pastoral)
- If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above
- Members of the school staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts
- All email communication between staff and members of the school community on school business must be made from an official school email account
- Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Headteacher
- Information that pupils and members of the wider community have access to as part of their involvement with South Wilts, including personal information, should not be discussed on their personal web space
- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media

accounts

- Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts
- We advise that school email addresses should not be used for setting up personal social media accounts or to communicate through such media
- The School accepts that some sites may be used for professional purposes to highlight a personal profile with summarised details, e.g. LinkedIn. The School would advise that care is taken to maintain an up to date profile and a high level of presentation on such sites if South Wilts is listed
- Staff who run blogging/microblogging sites which have a professional and/or educational status are advised to seek guidance and advice from assistant Headteacher e-safety, regarding prudence and endorsement of views if there is any link referencing South Wilts

3.2 School-sanctioned use of social media

3.2.1 There are many legitimate uses of social media within the curriculum and to support student learning. For example, the school has official Twitter accounts, and several A-level courses require the use of blogs for assessment. There are also many possibilities for using social media to enhance and develop students' learning.

3.2.2 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
- The content of any school-sanctioned social media site should be solely professional and should reflect well on the school
- Staff must not publish photographs of children without the written consent of parents/carers, identify by name any children featured in photographs, or allow personally identifying information to be published on school social media accounts
- 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
- Staff should not engage with any direct messaging of students through social media where the message is not public
- 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

4. 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.

5. 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 for staff and pupils.

Reviewed by	Date of Review / approval	Review cycle	Next Review Date	Statutory / Non statutory	Website
Resources	30.6.16 Updated 30.11.16	Annually	Summer 2017	Non-Statutory	Yes