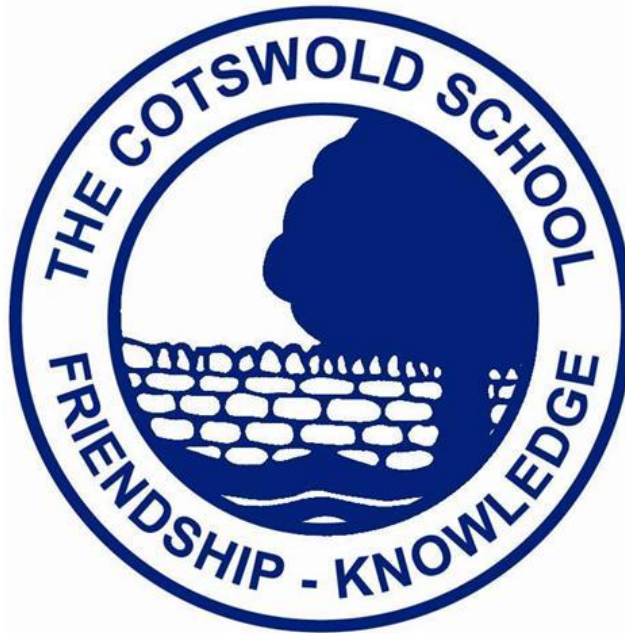




CSP POLICY 13

E Safety & Social Media Policy

Policy Author	JC/BE/ATh
Responsible Governors' Committee	Welfare & Wellbeing
Version number	11
Frequency of Review	2 years
Date of last Review	November 2025
Date approved by Governors	November 2025
Date of next review	November 2027

This policy is written and administered with due regard to our duty and commitment as a school to consider all aspects of equality and diversity.

Our E-Safety Vision:

As a School, we are dedicated to providing a safe environment for children, so they can focus on learning, growing and achieving, academically and socially.

The Internet and mobile technology are fantastic tools; our aim is to make sure students get the best use from them by educating them in using it safely and responsibly.

The Cotswold School recognises that clear E-Safety guidance and planning will help to ensure appropriate, effective and safer use of electronic communications.

End to End E-Safety

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

E-Safety at The Cotswold School depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students, encouraged by education and made explicit through published policies and taught lessons covering E-Safety.
- Sound implementation of E-Safety Policy in both administration and curriculum, including secure school network design and use.
- The continued supply of a safe and secure broadband connection from the South West Grid for Learning (SWGfL).
- Appropriate software tools (e.g. Impero) will be used at pupil workstation level to monitor all activity on the School network and to monitor and filter pupil activity on the internet.

Social media (e.g. Facebook, Twitter, Linked In) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube also have social media elements to them.

Staff, parents/carers and student/students will often use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation, as well as access to age-appropriate material. This policy section aims to encourage the safe use of social media by The Cotswold School, its staff, parents, carers and children.

This policy section is subject to the school's Codes of Conduct and Acceptable Use Agreements. It:

- Applies to all staff and to all online both professional and personal communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education

The school respects privacy and understands that staff and student/students and parents and carers may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Professional School Roles & Responsibilities

SLT

- Ensuring adequate online safety throughout the curriculum

- Developing and implementing the E-Safety and Social Media policy
- Taking a lead role in investigating any reported social media incidents

Administrator

- Create the account following SLT approval
- Store account details, including passwords securely
- Be involved in monitoring and contributing to the account
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Regularly monitoring, updating and managing content he/she has posted via the school administrator
- Adding an appropriate disclaimer to personal accounts when naming the school
- Anyone running a social media account on behalf of the school should read and understand this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

- School social media accounts – namely Facebook, X, LinkedIn and Instagram will be monitored regularly and frequently
- Any comments, queries or complaints made through those accounts will be responded to within 24 hours

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies and in line with KCSiE.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff and escalated where appropriate.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be

respected.

- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.

Personal use

Staff

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Students

- Staff are not permitted to follow or engage with current or prior student/students of the school on any personal social media network account.
- Student/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

Parents/Carers

Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff and escalated where appropriate.

E-Safety and the Prevent Duty

The school will protect children from the risk of radicalisation through the following procedures:

- Building students' 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
- Using the school's PSHE Tutor Programme and Personal Development lessons
- To explore sensitive and controversial issues
- To teach students to recognise and manage risk and make safer choices
- To recognise when pressures from others threatens their personal safety
- To teach different perspectives, develop questioning minds and to promote debate and challenging of extremist views
- Promote SMSC and British values
- Promote Internet Safety equipping children to stay safe on line through PSHE, ICT
- curriculum and the e-safety committee
- Promotion of CEOP as a way of reporting online concerns

Procedure if you have concern:

If the school staff are concerned that a student is vulnerable to radicalisation they will:

- Follow the school's normal safeguarding procedures
- Refer to the Channel programme
- The school will always liaise with other agencies – Local Safeguarding Partnership and the police.
- Any incidents or infringements of the E-Safety Policy will be investigated as soon as possible in a proportionate manner. For misuse that is not illegal, the procedures and sanctions in the relevant policies will be followed; for example the Behaviour, Acceptable Use, Anti-Bullying and Staff Disciplinary policies. Any illegal material or activities will be reported to the police and further liaison with any further support agencies will take place accordingly.
- See Appendix for e-safety related laws.

About this document

The E-Safety Policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole.

The School's E-Safety Policy forms part of the School Development Plan and operates in conjunction with other policies, including those for Child Protection and Safeguarding, Behaviour, Anti-Bullying, Sex and Healthy Relationships, Teaching & Learning, SMSC, Mobile Phone Usage Policy and Data Protection & the new general data Protection Regulations (GDPR), our Low-Level Concerns Policy and AI Policy.

- This Policy has been drafted in consultation with Wellbeing and Welfare Committee.
- The School E-Safety Lead Professional sits on this Committee (Jodi Carter, DSL & Deputy Headteacher).
- The Committee includes staff, students, parents, the School's Designated Safeguarding Lead and the E-Safety Governor.
- The E-Safety Policy and its effectiveness will be reviewed every 2 years.
- It has been agreed by the Senior Leadership Team and approved by Governors.
- The Governing Body will receive a regular report on the implementation of this Policy from the E-Safety committee via the E-safety Governor.
- The School will monitor the impact of the Policy using:
 - Logs of reported incidents
 - SWGfL monitoring logs of internet activity (including sites visited)
 - Internal monitoring data for network activity via Impero
 - Surveys of
 - students
 - parents/carers
 - staff

Teaching And Learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The School has a duty to provide students with high quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

Internet use will enhance learning

- The School Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The Internet allows students to explore different cultures and world views, enhancing their development as social, moral, cultural and spiritual citizens.

Students will be taught how to evaluate Internet content

- Schools should ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- 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 be taught how to keep themselves safe online from images and disturbing content.

Managing ICT at The Cotswold School

Information system security

- School ICT systems capacity and security will be reviewed regularly, in conjunction with SWGfL.
- The School will be responsible for ensuring that the School network is as safe and secure as is reasonably possible.
- Virus and malware protection will be installed and updated regularly.
- All users will have clearly defined access rights to School ICT systems.

- Managing filtering
- The School will work in partnership with SWGfL in monitoring all content when accessing the internet or other ICT related tasks, ensuring that it is age-appropriate.
- If staff or students discover an unsuitable site, it must be reported to the ICT Network Manager.
- ICT staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Managing videoconferencing
- Videoconferencing will be appropriately supervised for all students.
- Managing emerging technologies
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.
- Managing personal devices
- The Acceptable Use Policy encompasses personal electronic devices.
- The Mobile Phone Policy outlines the School's approach to managing the widespread pupil ownership of these devices. It will be reviewed regularly.
- Any electronic devices brought to School are the responsibility of the owner; the School accepts no responsibility for loss, theft or damage to such items.
- The School's wireless network will not be available to students for mobile use, except to 6th Form students who have agreed to the 6th Form BYOD policy and received written permission.
- The use of mobile technology to send abusive or inappropriate text messages or email is forbidden, as is the videoing or photographing of others without permission.
- With the exception of devices permitted by 6th Form BYOD and AUP agreements, personal mobile devices may only be used in lessons as part of teaching the curriculum and this use requires the approval of the Principal or a member of Senior Leadership Team – not even within Key Stage 3
- Protecting personal data
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) May 2018
- Personal or sensitive data may only be accessed remotely or taken off-site with the approval of the Principal or a member of Senior Leadership Team. It must be encrypted.
- E-mail
- All Students and Staff have a network account and an individual email address.
- Students are responsible for all content sent from their e-mail account.
- Students must immediately tell a teacher if they receive offensive e-mail in school.
- Students must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully, in the same way as a letter written on School headed paper.
- The forwarding of chain letters is not permitted.
- Remote File Access - Foldr (School Portal) is used to allow staff, and students, access to their files and resources saved in school, from internet enabled devices.
- Use of Foldr (School Portal) is governed by the Acceptable Use Policy.
- Usage will be monitored to ensure that guidelines are effective.

Published content and the School website

The contact details on the School website include the School address, e-mail and telephone number. Staff or pupil personal information is not published, although pictures of students may be accessible.

The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate. The Principal can delegate editorial responsibility to the qualified staff member who oversees the school's online presence on a daily basis.

Publishing a pupil's image and work

- Photographs that include students will be selected carefully and will only enable individual students to be clearly identified, where written permission has been obtained from parents/carers.

- Written authority will be sought from parents/carers for photographs of students to be published on the School website and in other School publications.
- A pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- Access to social networking sites, such as Facebook, Twitter, Instagram, Snapchat, Whatsapp and chat-rooms, will either be blocked or access will be filtered. Newsgroups will be blocked, unless a specific use is approved.
- YouTube will not be available for students but may be available to teachers' accounts in a classroom.
- Staff may seek permission from the Senior Leadership team and Safeguarding Lead for exceptional access to the above areas for specific curriculum needs.
- Students will be advised on security and never to give out personal details of any kind which may identify them or their location.
- Students will be advised to set strong passwords, to deny access to both known and unknown individuals and to know how to block unwanted communications.

Cyber-bullying

- The School recognises the impact of cyber-bullying on the academic achievement of its young people and on their development as spiritual, moral, social and cultural members of the community. The entire school community is made aware of the responsibilities involved in the use of technology and the potential impact of cyber-bullying on individuals.
- The School actively encourages the entire School community to be vigilant about the risks posed by mobile and wireless technology, through its ongoing & up to date E-Safety education programme for students, staff, governors and parents.
- The School recognises its inability, beyond the comparative safety of the School's ICT network, to control the actions of its students in cyberspace. However, the School's Behaviour and Anti-Bullying policies apply equally to cyber-bullying.
- Even if cyber-bullying incidents occur outside the School whether by way of texting, videoing or taking photographs, if they are reported, the School will endeavour to investigate and resolve matters in line with relevant policies, thereby acknowledging the impact it can have on individuals and friendship groups within school.
- The School provides an online anonymous reporting mechanism to enable students to report any incidents or concerns. This is currently in the form of an E-Safety/bullying 'button' on the front of the school intranet. It is clearly visible and accessible to all students. Any matters raised in this way are dealt with in the same manner as other reports.
- The school also has a link to the Child Exploitation Online Protection Service (CEOP) Advice, Help, Report Abuse button

Sexting

- The term 'sexting' is used to describe the sending and receiving of sexually explicit photos, messages and video clips, by text, email or posting them on social networking sites.
- The school is mindful of the fact that young people have no control over how and where images and messages might be shared online by others and that sexting can leave them vulnerable to bullying, humiliation and embarrassment, or even to blackmail. The school recognises that young people may see sexting as a harmless activity but is aware that taking, sharing or receiving an image can have a long-lasting impact on someone's self-esteem.
- The school acknowledges that sharing of inappropriate content can lead to negative comments and bullying and can be very upsetting and that explicit content can spread very quickly over the internet and have a negative effect on a student's reputation both inside and outside school. It is mindful that it could also affect their education and employment prospects.
- In addition, the school is mindful that when young people engage in sexting they are creating an indecent image of a person under the age of 18 which, even if taken by themselves, is against the law. Distributing an indecent image of a child such as sending it by text is also illegal. The Police will always be informed.
- As a result, the school will take all reports of sexting very seriously. Matters will be fully investigated and students and parents will be involved and supported as appropriate, including via external agencies.

Child on Child Abuse Online

- The determination of whether behaviour is developmental, inappropriate or abusive will hinge around the related concepts of true consent, power imbalance and exploitation.
- The school recognises that there may be a need for some form of behaviour management or multi-agency intervention to deal with the negative effects of inappropriate sexual behaviour online.
- Abusive sexual activity online includes any behaviour involving coercion, threats, aggression together with secrecy, or where one participant relies on an unequal power base

POLICY DECISIONS

Authorising ICT and Internet access

- All staff must read and sign the Acceptable Use Policy before using any School ICT resources.
- The School will maintain a current record of all staff and students who are granted access to School ICT systems.
- Access to ICT resources and/or the internet will be withdrawn should the system be used inappropriately.
- Any visitor given access to the School's ICT systems will be required to read and sign the Acceptable Use Policy.

Assessing risks

- The School will take all reasonable precautions to prevent access to inappropriate material.
- However, due to the global and connected nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a School computer.
- Neither the School nor its staff can accept liability for the material accessed or any consequences of Internet access.
- Where students are undertaking off-site educational activities, the risk assessment procedure will consider E-Safety issues and guidance as per the policy will be given
- The School will audit ICT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate.

Handling E-Safety incidents

- Concerns about E-Safety, including cyber-bullying, will be dealt with initially by the Safeguarding Team, with the involvement of a member of the Senior Leadership team, as necessary.
- Complaints will be dealt with according to the Complaints Procedure Policy. Any complaint about staff misuse must be referred to the Principal.
- Incidents impacting Child Protection will be dealt with in accordance with the Child Protection Policy.
- Gloucestershire Police advice will be sought on potentially illegal issues.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Gloucestershire Police.

Acceptable User Policies & related documents

- AUPs will be kept as separate, but related documents to facilitate regular and ongoing updates.
- A Glossary of E-Safety contacts and details of the legislative framework will be maintained separately, to enable them to be kept up-to-date

Communications

Policy Introducing the E Safety Policy to students

- Students will be asked to read, agree and sign the Acceptable Use Policy.
- E-Safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored.
- E-Safety training and guidance underpins all cross-curricular and subject use of the internet.
- Students will receive E-safety updates as appropriate via PHSE sessions and in their Personal Development lessons.

Staff and the E-Safety Policy

- This Policy will be presented to all members of staff.
- Staff will be asked to read, agree and sign the Acceptable Use Policy.

- The school will provide staff with up to date and regular E-Safety information by way of email and on Inset Days, regarding safe and responsible Internet use, both professionally and
- personally. This will include current national trends and general matters arising in school.
- E-Safety (including WRAP) training will be provided as part of the induction programme for new staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Data is regularly logged to this effect.
- Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.

Enlisting parental support

- Parents' attention will be drawn to this E-Safety Policy in newsletters, the School prospectus and on the School website, Facebook and Twitter.
- Parents will be asked to read the Acceptable Use Policy for Students and to confirm their support as part of the Home School Agreement.
- The abbreviated parent version of the Anti-Bullying Policy includes a section on cyber- bullying.
- E-safety information will regularly be provided by way of parent mail, newsletters and at Information Evenings and there will be liaison with local Primary Schools.
- Students will be encouraged to share their E-Safety awareness with their families