THE COTSWOLD SCHOOL E – SAFETY POLICY DOCUMENT

Policy:	**E-Safety Policy**
Policy Ref:	**CSP 13**
Version Number:	**4.0**
Date:	**Oct 2018**
Review Date:	**Sept 2019**
Authorised by:	**Governing Body**
Updated by:	**Mrs L Rowley (E-Safety Governor), Mrs J Carter (Designated Safeguarding Lead) and Mrs F Peake (E-Safety Lead Professional)**

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 pupils 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 pupils, 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.

E-Safety and the Prevent Duty

All teaching staff received WRAP training in February 2016.

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

- Building pupils' 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 and tutor programme:
- To explore sensitive and controversial issues
- To teach pupils 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

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 Board 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 User and 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).

- This Policy has been drafted in consultation with the E-Safety Committee.
- The School E–Safety Lead Professional chairs the E-Safety Committee.
- The Committee includes staff, pupils, parents, the School's Designated Safeguarding Lead and the E-Safety Governor.
- The E–Safety Policy and its effectiveness will be reviewed annually.

- 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
        - pupils
        - parents/carers
        - staff

1. 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 pupils 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 pupils.

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 pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The Internet allows pupils to explore different cultures and world views, enhancing their development as social, moral, cultural and spiritual citizens.

Pupils will be taught how to evaluate Internet content

- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be made aware of how to keep themselves safe online from images and disturbing content.

2. 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 pupils 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 pupils.

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 pupils 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.

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 Pupils and Staff have a network account and an individual email address.
- Pupils are responsible for all content sent from their e-mail account.
- Pupils must immediately tell a teacher if they receive offensive e-mail in school.
- Pupils 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

- Magellan (School Portal) is used to allow staff, and students, access to their files and resources saved in school, from internet enabled devices.
- Use of Magellan (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 pupils 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 pupils will be selected carefully and will only enable individual pupils to be clearly identified, where written permission has been obtained from parents/carers.
- Written authority will be sought from parents/carers for photographs of pupils 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 pupils, but may be available to teachers' accounts in a classroom.
- Staff may seek permission from the Senior Leadership team for exceptional access to the above areas for specific curriculum needs.
- Pupils will be advised on security and never to give out personal details of any kind which may identify them or their location.
- Pupils 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 pupils, 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 pupils 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 pupils 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 (CEOPS) 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 recognises that it is practised by young people who send images and messages to their friends, or even strangers they meet online.
- The school recognises that there are a variety reasons why a young person might get involved in sexting. Exploring sex and relationships is a natural part of adolescence. Young people often feel that they love and trust their partner and want to express their sexual feelings.
- The school is aware that sometimes, young people might be put under pressure to either take pictures of themselves or forward those taken by others. They may want to please a demanding boyfriend or girlfriend, or do what they think everyone else is doing. Or they may have been persuaded by an adult or someone they've met online.
- 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 school appreciates that it is unlikely that a child or young person would be prosecuted for a first offence, but it is possible that the police might want to investigate.
- 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.

Peer on Peer Abuse Online

- It is recognised that the boundary between what is abusive online and what is part of normal childhood or youthful development and experimentation can be blurred.
- 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 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.

3. 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 pupils 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 pupils 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 E-Safety Lead Professional, with the involvement of a member of the Senior Leadership team, as necessary. An incident log will be maintained, including details of action taken. This log will be inspected on at least 3 occasions in the school year, by the E-Safety Governor.
- 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.

Community use of the Internet

- The School will liaise with local organisations to establish a common approach to E-Safety.

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

4. COMMUNICATIONS POLICY

Introducing the E-Safety Policy to pupils

- Pupils will be asked to read, agree and sign the Acceptable Use Policy.
- E-Safety rules will be posted in all networked rooms.
- Pupils 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 PSHE days and in tutor time

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 Pupils 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.
- Pupils will be encouraged to share their E-Safety awareness with their families.

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.

(08/10/2018)

ratified by Governors and
signed as such by The Chair of Governors