E-SAFETY and INTERNET USE POLICY

The following policy incorporates the best advice offered to the School by:

- the government through its recently established Superhighway Safety website,
- the Wiltshire Education and Libraries Department,
- the National Association for Co-ordinators and Teachers of IT and
- other schools with effective and definitive policies structures in place.

The E-Safety and Internet Policy is intended to cover the rights and responsibilities of:

- students,
- teachers, classroom assistants, technicians,
- parents/guardians,
- those responsible for designing and maintaining the School's web site

It must be noted that whilst that this policy is intended to provide a clear code of conduct for all users, changes in this field are very rapid.

This policy should be read in conjunction with specific school rules on:

- access authorisation,
- safeguards covering personal information (especially under the Data Protection Act),
- limitations on use by staff and students,
- protocols for use outside timetabled lessons such as those pertaining to the School's computer club or visiting organisations,
- web sites which are prohibited either by SWGFL or the School,
- guidance on downloading materials that may be virus contaminated,
- guidance on copyright,
- the role of the Headteacher or designated person with delegated responsibility for the School's local area network.
- The schools bullying policy.

Section 1 – Student Access

1 All students have access to the Internet through classroom workstations and have sole responsibility for the security of their own passwords.

2 All students have further privileges to Internet and possibly E-mail facilities at lunch times or after school on the condition that their parents/guardians have signed the form ICT 1 on ***Responsible Internet Use***.

3 Students must be supervised at all times when accessing the Internet. Unacceptable uses of the Internet are regarded as :

- Students posting personal information about themselves or other people, especially contact information such as addresses or telephone numbers.
- Students attempting to log-on to the School's network or the Internet via an unauthorised account. (Students may only use their own accounts)
- Students attempting to download any programs or materials from the Internet without prior permission from the School's IT and Computing Subject leader, network manager or their class teacher
- Students using language judged by the School's IT and Computing Subject leader or Network Manager to be damaging, disruptive, obscene, prejudicial, discriminatory, harassing, distressing, annoying or injurious in any way.
- Students breaching *any area* of copyright including music.
- Students accessing, or attempting to access any inappropriate websites relating to criminal activity, pornography, indecent images or other unsuitable or unseemly material, to include any website associated with extremist or terrorist organisations.
- Students attempting to access websites associated with the radicalisation of young people.
- Students attempting to access websites which undermine Fundamental British Values including democracy, the rule of law, individual liberty and mutual respect and tolerance of others with different faiths and beliefs.
- Students misusing the ICT network for non educational activities, such as on line interactive games or internet shopping.
- Students accessing social networking sites that are not approved by the school. This includes Facebook.

Other Technologies

The emergence of new technologies will be closely monitored to assess the impact that these might have on both educational benefits and any potential harm that they may cause. Currently:

- Students will not use mobile phones to convey inappropriate messages or images and the **taking of images of any other student or member of staff is strictly forbidden** either during lessons or during social time.
- Students will not use mobile phones as part of the lesson unless specifically allowed to do so by their teacher
- Students will not access or attempt to access internet websites which are designed to circumvent site which have been filtered by the school or associated organisations.

- Students wishing to use their own laptop computers or similar devices must first seek the permission of the network manager.
- Students will not connect any portable device to the schools computer network without permission from the network manager

Section 2 – Staff Access

1 All staff have controlled access to the School's local area network and the Internet via any of the School's workstations.

2 Staff are assigned E-mail addresses and may subscribe to other external agencies if they so choose.

Unacceptable uses of the Internet by staff are regarded as, for example,

- Attempting to gain unauthorised access to, or browsing, any other computer system beyond their authorised school account.
- Downloading programs or files without the permission of the School's ICT Co-ordinator or the ICT Technician.
- Using language judged to be inappropriate by the School's IT and Computing Subject leader, Network Manager or member of the SMT, or language judged by the same to be damaging, disruptive, obscene, prejudicial, discriminatory, harassing, distressing, annoying or injurious in any way; or knowingly or recklessly posting false or defamatory information about a person or organisation.
- Posting private messages without permission of the person to whom the message was sent.
- Posting private information about another person.
- Plagiarism or breach of copyright.
- Accessing profane or obscene materials, or any materials that advocate illegal acts, violence, discrimination or hate against another person.

Staff will at all times supervise any children to whom they authorise access to the School's local area network or the Internet.

If children access inappropriate materials there are two courses of action:

1 Children must be immediately removed from the computer they are working at and have their computer access privileges suspended according to the discretion of the ICT Co-ordinator.

2 Any child will have their computer immediately closed down if the supervising teacher judges they have accessed inappropriate materials accidentally. It should be reported as soon as is possible to the School's IT and Computing

Subject leader, Network Manager or member of the SMT. All incoming and outgoing E-mail should be screened by any supervising teacher.

It should be remembered that the school intranet is the property of The Stonehenge School and remains so at all times.
Each person's user area is stored on the main server and a log of each person's ICT activity is kept on a daily basis.
Although this is not routinely inspected, where it is believed that there has been inappropriate use or misuse of the ICT network, by either staff or student, a person's user area can be accessed by either the Headteacher or the Network Manager in consultation.
Where appropriate, this may be reported directly to the Chair of Governors and appropriate action taken.

Section 3 – The School Web Site

The new Stonehenge School Web Site came on line in 2011. Its purpose is to positively promote the image of the School to the world at large and in doing so will seek *to " . . . balance the potential risks of including images of pupils on the web site against the design principles of creating colourful, attractive and relevant pages, as the School, the head and the governors would do with any publication."*
(Superhighway Safety – safe use of the Internet statement)

To this end the School will seek to ensure that:

- A student's name is never published alongside a photograph.
- If a contact person is needed for a project that person will be a teacher and not a student.
- No identifying materials will be posted on the Internet, such as personal telephone numbers or addresses.
- If class or group pictures are posted names may be mentioned but not in the order in which individuals are standing in any picture.
- Class pictures will generally include at least three students.
- If individual pictures are posted of students their names will not be included.
- Personal web pages will not be published from school. Where a web page is published it will be based on classroom curricula.
- No video footage of pupils will be published under any circumstances

Any correspondence via E-mail with staff or students at the School will be through the School's official address at *admin@stonehenge.wilts.sch.uk* and no other address. Any use of E-commerce must be sanctioned by the Headmaster and the governors.

Where judged to be appropriate by the Headmaster or the governors any breach of the above conditions may be referred to the Wiltshire County Council or the Governing Body for further action. Standard disciplinary procedures may be sanctioned when necessary.

Every user is asked to agree to this policy, every time they log on to a machine on the school network.

Adopted	September 2014
Review	September 2015