Saffron Walden County High School

E-Safety Policy

Date adopted or ratified; 2nd November 2015
Review Date; July 2019
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>POLICY GUIDANCE</td>
<td>4</td>
</tr>
<tr>
<td>POLICY MONITORING AND UPDATING</td>
<td>5</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>6</td>
</tr>
<tr>
<td>SCOPE OF THE POLICY</td>
<td>7</td>
</tr>
<tr>
<td>ROLES AND RESPONSIBILITIES</td>
<td>8</td>
</tr>
<tr>
<td>EDUCATION</td>
<td>12</td>
</tr>
<tr>
<td>MONITORING</td>
<td>15</td>
</tr>
<tr>
<td>BREACHES</td>
<td>16</td>
</tr>
<tr>
<td>INCIDENT REPORTING</td>
<td>17</td>
</tr>
<tr>
<td>INCIDENT REPORTING – RADICALISATION</td>
<td>19</td>
</tr>
<tr>
<td>COMPUTER VIRUSES</td>
<td>20</td>
</tr>
<tr>
<td>DATA SECURITY INTRODUCTION</td>
<td>21</td>
</tr>
<tr>
<td>SCHOOL SECURITY POLICY</td>
<td>24</td>
</tr>
<tr>
<td>IMPACT LEVELS AND PROTECTIVE MARKING</td>
<td>25</td>
</tr>
<tr>
<td>DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY</td>
<td>27</td>
</tr>
<tr>
<td>E-MAIL POLICY</td>
<td>21</td>
</tr>
<tr>
<td>MANAGING THE SCHOOL E-SAFETY MESSAGES</td>
<td>24</td>
</tr>
<tr>
<td>DEALING WITH AN E-SAFETY INCIDENT GUIDELINES</td>
<td>25</td>
</tr>
<tr>
<td>INTERNET ACCESS POLICY</td>
<td>27</td>
</tr>
<tr>
<td>MANAGING OTHER WEB 2.0 TECHNOLOGIES POLICY</td>
<td>30</td>
</tr>
<tr>
<td>PARENTAL INVOLVEMENT POLICY</td>
<td>33</td>
</tr>
<tr>
<td>PASSWORDS AND PASSWORD SECURITY POLICY</td>
<td>34</td>
</tr>
<tr>
<td>PERSONAL INFORMATION PROMISE</td>
<td>36</td>
</tr>
<tr>
<td>PERSONAL OR SENSITIVE INFORMATION POLICY</td>
<td>37</td>
</tr>
<tr>
<td>REMOTE ACCESS POLICY</td>
<td>38</td>
</tr>
<tr>
<td>SAFE USE OF IMAGES AND VIDEO POLICY</td>
<td>39</td>
</tr>
<tr>
<td>SCHOOL ICT EQUIPMENT INCLUDING PORTABLE &amp; MOBILE ICT EQUIPMENT</td>
<td>42</td>
</tr>
<tr>
<td>SERVERS POLICY</td>
<td>45</td>
</tr>
<tr>
<td>SMILE AND STAY SAFE POSTER</td>
<td>46</td>
</tr>
<tr>
<td>SYSTEMS AND ACCESS POLICY</td>
<td>47</td>
</tr>
<tr>
<td>TELEPHONE SERVICES POLICY</td>
<td>48</td>
</tr>
<tr>
<td>CURRENT LEGISLATION</td>
<td>49</td>
</tr>
<tr>
<td>APPENDIX 1: ACCEPTABLE USE AGREEMENT: STUDENT - SECONDARY</td>
<td>53</td>
</tr>
<tr>
<td>APPENDIX 2: ACCEPTABLE USE AGREEMENT: STAFF, GOVERNORS AND VISITORS</td>
<td>56</td>
</tr>
<tr>
<td>APPENDIX 3: CURRICULUM E-SAFETY</td>
<td>58</td>
</tr>
<tr>
<td>APPENDIX 4: USE OF STAR LESSON VIDEO EQUIPMENT</td>
<td>59</td>
</tr>
<tr>
<td>APPENDIX 5: BYOD POLICY – SIXTH FORM</td>
<td>60</td>
</tr>
</tbody>
</table>
APPENDIX 6: SWCHS TWITTER GUIDANCE FOR STUDENTS ............................................. 63
APPENDIX 7: SWCHS TWITTER GUIDANCE FOR STAFF .................................................. 64
APPENDIX 8: BYOD POLICY YEARS 7-11 ........................................................................ 65
APPENDIX 9: E-SAFETY GROUP TERMS OF REFERENCE ............................................. 66
APPENDIX 10: FURTHER READING ............................................................................... 69
APPENDIX 11: FORMS AND TEMPLATES ..................................................................... 72
Policy Guidance

This e-safety policy has been developed and approved by:

- Headteacher & Senior Leaders
- Director of ICT as E-Safety Co-ordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governing Body
- Digital Leaders (students)
- Parents

Consultation with the whole school community has taken place through a range of formal and informal meetings.

There will be an on-going opportunity for staff to discuss with the E-Safety coordinator any issue of E-Safety that concerns them.

There will be an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them.
## Policy Monitoring and Updating

<table>
<thead>
<tr>
<th>This e-safety policy was approved by the Governing Body on:</th>
<th>2(^\text{nd}) November 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>The implementation of this e-safety policy will be monitored by the:</td>
<td>E-Safety Coordinator</td>
</tr>
<tr>
<td>Monitoring will take place at regular intervals:</td>
<td>Annually</td>
</tr>
<tr>
<td>The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:</td>
<td>Once per term</td>
</tr>
<tr>
<td>The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:</td>
<td>November 2019</td>
</tr>
<tr>
<td>Should serious e-safety incidents take place, the following external persons / agencies should be informed:</td>
<td>Safeguarding Lead, Deputy Safeguarding Lead &amp; PREVENT Lead, Police Community Support Officer</td>
</tr>
</tbody>
</table>

### The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of Internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of:
  - students
  - parents / carers
  - staff
Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Saffron Walden County High school we understand the responsibility to educate our students on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).
Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.
Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

**Governing Body:**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor in combination with responsibility for safeguarding.

The role of the E-Safety Governor will include:

- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

**Headteacher and Senior Leaders:**

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator. Serious concerns will be shared with the Safeguarding governor.

The Headteacher and (at least) another member of the Senior Leadership should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR disciplinary procedures).

The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring.

The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

**E-Safety Co-ordinator:**

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Safeguarding Lead in school and other external agencies as appropriate.
- Liaises with school technical staff.
• Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

• Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs

• Attends relevant meeting of Governors

• Reports regularly to Senior Leadership Team

**Network and Manager ICT Support Team:**

The Network Manager and ICT Support Team are responsible for ensuring:

• That the school’s technical infrastructure is secure and is not open to misuse or malicious attack.

• That the school meets required e-safety technical requirements and any Local Authority E-Safety Policy that may apply.

• That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

• The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

• That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

• That the use of the network / Internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher, Safeguarding Officer and E-Safety Coordinator for investigation / action / sanction.

• That monitoring software / systems are implemented and updated as agreed in school policies.

**Teaching and Support Staff**

Are responsible for ensuring that:

• They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.

• They have read, understood and signed the Staff Acceptable Use Policy.

• They report any suspected misuse or problem to the Headteacher, Safeguarding Officer and E-Safety Coordinator for investigation / action / sanction.

• All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems.

• E-safety issues are embedded in all aspects of the curriculum and other activities.

• Students understand and follow the e-safety and acceptable use policies.

• Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
• They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

• In lessons where Internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

**Safeguarding Lead**

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

(NB: it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop)

**E-Safety Group**

The E-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The E-safety group will be part of the Safeguarding group once a term.

Members of the E-safety will assist the E-Safety Coordinator with:

- The production / review / monitoring of the school e-safety policy and related documents.
- The production / review / monitoring of the school filtering policy and requests for filtering changes.
- Mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression.
- Monitoring network / Internet / incident logs.
- Consulting stakeholders – including parents / carers and the students about the e-safety provision.
- Monitoring improvement actions identified.

**Students**

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

• Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

• Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

• Digital and video images taken at school events.

• Access to parents’ sections of the website and on-line student / student records via third party websites.

• Their children’s personal devices in the school (where this is allowed).

• Discussion about the school and its staff on social media.

Community Users

Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User Agreement before being provided with access to school systems.
Education

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of Students in e-safety is therefore an essential part of the school’s e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

• A planned e-safety curriculum should be provided is part of Computing / PHSE / other lessons and should be regularly revisited. See appendix three for details of provision within these subjects.

• Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.

• Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

• Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

• Students should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

• Staff should act as good role models in their use of digital technologies the Internet and mobile devices.

• In lessons where Internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

• Where students are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the young people visit.

• It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the ICT Support Team can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

• Educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.

• Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
Students with Additional Needs:

- The school endeavors to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools’ E-Safety rules.

- However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

- Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities

- Letters, newsletters, web site

- Parents / Carers evenings

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school’s e-safety knowledge and experience. This may be offered through the following:

- E-Safety messages targeted towards grandparents and other relatives as well as parents.

- The school website will provide e-safety information for the wider community.

- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision.

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use
Agreements.

- The E-Safety Co-ordinator will receive regular updates through attendance at external training and by reviewing guidance documents released by relevant organisations.

- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

- The E-Safety Co-ordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub group / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.

- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).
Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, Internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All Internet activity is logged by the school’s Internet provider. These logs may be monitored by authorised staff.
Breaches

A breach or suspected breach of policy by a School employee, contractor or student may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the Essex County Council Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.
Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school’s E-Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your SIRO.

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Complaints and/ or issues relating to E-Safety should be made to the E-Safety co-ordinator or Headteacher. Incidents should be logged and the Essex Flowcharts for Managing an E-Safety Incident should be followed.

Inappropriate Material:

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Safety Co-ordinator and Safeguarding Officer.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety Co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of ‘grooming’ behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
• Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.
Incident Reporting – Radicalisation

Terrorist organisations, such as ISIL, are trying to radicalise and recruit young people through an extensive use of social media and the internet. Young people, some as young as 14, have tried to leave the UK to travel to join ISIL and other terrorist groups in Syria and Iraq. As with other online harms, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

Schools have a vital role to play in protecting pupils from the risks of extremism and radicalisation. Keeping children safe from risks posed by terrorist exploitation of social media should be approached in the same way as safeguarding children from any other online abuse.

- In the same way that teachers are vigilant about signs of possible physical or emotional abuse in any of their pupils, if you have a concern for the safety of a specific young person at risk of radicalisation, you should follow your school’s safeguarding procedures, including discussing with your school’s designated safeguarding lead, and where deemed necessary, with children’s social care.

- You can also contact your local police force or dial 101 (the non-emergency number). They can talk to you in confidence about your concerns and help you gain access to support and advice.

- The local authority or police might suggest a referral to the ‘Channel’ programme. ‘Channel’ is a voluntary Government funded programme which aims to safeguard children and adults from being drawn into terrorist activity. ‘Channel’ can provide a support plan and specific interventions to protect people at risk, including mentoring support or an ideological or theological intervention. If you want to find out more about ‘Channel’ click here or call 101 to discuss your concerns.

- If you are concerned that a child’s life is in immediate danger, or that they may be imminently planning to travel to Syria or Iraq dial 999 or call the confidential Anti-Terrorist Hotline on 0800 789 321.

For further background information on the roles of schools and teachers in safeguarding children, and preventing pupils from the risks of terrorism and extremism please follow this link:

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD) must be checked for any viruses using school provided anti-virus software before using them.

- Never interfere with any anti-virus software installed on school ICT equipment that you use.

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.
E-Mail Policy

The use of e-mail within most schools is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and good network etiquette; ‘netiquette’.

Staff: Please also see staff code of conduct policy for specific staff guidance on e-mail use.

Managing E-Mail:

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.

- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses.

- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, ‘the views expressed are not necessarily those of the school or the LA’.

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

- Staff sending e-mails to external organisations, parents or students are advised to cc. the Headteacher, line manager or designated account if the email is of a sensitive nature.

- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- All student e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

- Students must immediately tell a teacher/trusted adult if they receive an offensive e-mail.

- Staff must inform the E-Safety Co-ordinator if they receive an offensive e-mail.

- Students are introduced to e-mail as part of the Computing Scheme of Work.
• However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

• The use of any other Internet based webmail service for sending, reading or receiving business related e-mail is not permitted.

Sending E-mails:

• If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section Error! Reference source not found..

• Use your own school e-mail account so that you are clearly identified as the originator of a message.

• Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

• Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

• An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail.

• School e-mail is not to be used for personal advertising.

Receiving e-Mails:

• Check your e-mail regularly.

• Activate your ‘out-of-office’ notification when away for extended periods.

• Never open attachments from an untrusted source; Consult your network manager first.

• Always report communication that is offensive or makes you feel uncomfortable to your line manager.

E-mailing Personal, Sensitive, Confidential or Classified Information:

• Assess whether the information can be transmitted by other secure means before using e-mail. E-mailing confidential data is not recommended and should be avoided wherever possible.

• The use of Internet based webmail service for sending e-mail containing sensitive information is not permitted.

• Where your conclusion is that e-mail must be used to transmit such data:
  o Obtain express consent from your manager to provide the information by e-mail
  o Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    o Verify the details, including accurate e-mail address, of any intended recipient of the information
    o Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    o Do not copy or forward the e-mail to any more recipients than is absolutely necessary
    o Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document attached to an e-mail
- Provide the encryption key or password by a separate contact with the recipient(s) – preferably by telephone
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

- Essex Police
- District and Borough Councils within Essex County Council
- Essex NHS Trusts
Managing the School E-Safety Messages

- We endeavor to embed E-Safety messages across the curriculum whenever the Internet and/or related technologies are used.
- The E-Safety policy will be introduced to the students at the start of each school year.
- E-Safety posters will be prominently displayed.
- There will be regular E-Safety messages to students as incidents occur.
- Parents will be invited to an e-safety evening.
Dealing with an E-Safety Incident Guidelines

**Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an illegal e-safety incident**

Following an e-safety incident a decision will have to be made quickly as to whether the incident involved any illegal activity.

Examples of illegal activity would include:
- Downloading abusive images
- Passing child pornography to others
- Inciting racist or religious hatred
- Extreme cases of cyberbullying
- Promoting illegal acts

Still unsure?
For further advice ECC ISIS helpdesk on 01245 431851 or Essex Police on 0300 333 4444

Has illegal activity taken place?

- YES
  - Inform Essex Police and Essex County Council
  - Follow the advice given by the Police, or
  - Confiscate the device and if related to the school network disable user account
  - Save ALL evidence but DO NOT view or copy.
  - If a pupil is involved contact Social Care Direct to make an emergency referral on 0845 603 7634
  - If it involves a member of staff contact the LADO on 01245 436744

- NO
  - Go to next flowchart which outlines the process for non-illegal incidents

Users must be aware that if they find something unpleasant or frightening they should switch off their screen or close the laptop and talk to a member of staff.

**Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an e-safety incident where no illegal activity has taken place**

If a member of staff has:
1. Behaved in a way that has, or may have, harmed a child
2. Possibly committed a criminal offence
3. Behaved towards a child in a way that indicates that he/she may be unsuitable to work with children Contact LADO on 01245 436744
   - Review evidence and determine whether the incident was accidental or deliberate
   - Decide upon the appropriate course of action
   - Follow school disciplinary procedures (if deliberate) and contact Schools HR on 01245 436120 or your schools Link Officer
   - Support the pupil by one or more of the following:
     - Class Teacher
     - e-Safety Co-ordinator
     - Headteacher/Senior Leader
     - Designated Child Protection Officer
     - School PCSO

   Inform Parent/carer as appropriate
   - If the child is at risk contact Social Care Direct to make an emergency referral on 0845 603 7634

Incident types could be:
- Using another persons user name or password
- Accessing websites which are against the schools policy e.g. gaming
- Using a mobile phone to take video during a lesson
- Using technology to upset or bully

The Headteacher/e-Safety Co-ordinator should:
- Record the incident in the e-safety log
- Keep any evidence

Did the incident involve a member of staff?

- YES
  - Pupil as Victim
  - Pupil as Instigator

- NO
  - Was the Child the victim or perpetrator?
  - Pupil as Victim
  - Pupil as Instigator

Review incident to decide if other pupils were involved
- Decide appropriate sanctions
- Inform Parent/Carer if serious or persistent incident
- If serious, consider informing the Duty Safeguarding Officer as the child instigator could be at risk.
Internet Access Policy

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so; because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school’s filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to the E-Safety once every term, in the form of an audit of the change control logs

All users have a responsibility to report immediately to the Network Manager any infringements of the school’s filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements:

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists.

Filter content lists are regularly updated and Internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed Internet access through the school network, filtering will be applied that is consistent with school practice.

The school has provided enhanced / differentiated user-level filtering through the use of the Lightspeed filtering programme. (Allowing different filtering levels for different ages / stages and different groups of users – staff / students etc.)

In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher or other nominated senior leader).

Mobile devices that access the school Internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems

Any filtering issues should be reported immediately to the filtering provider.
Requests from staff for sites to be removed from the filtered list will be considered by the technical staff and E-Safety Co-ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group.

**Education / Training / Awareness:**

Students will be made aware of the importance of filtering systems through the e-safety education programme (see previous section on education). They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school’s filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

**Changes to the Filtering System:**

- Staff can request a change to the schools filter system (allow a blocked site) by raising a support ticket containing the URL of the site and the educational reason for the change.
- Similarly, if a request for a site to be blocked is made, the same procedure applies and the reason for the block should be cited.
- The changes should be logged by the network support team and supervised by the network manager. Any queries regarding changes should be directed to the E-Safety Co-ordinator.
- The log should be provided once a term to the E-Safety Co-ordinator to be audited at an E-Safety group meeting.

**Monitoring:**


- Staff and students are aware that school based email and Internet activity can be monitored and explored further if required
- The school does not allow students access to Internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

**Audit / Reporting:**
Logs of filtering change controls and of filtering incidents will be made available to:

- E-Safety Co-ordinator
- E-Safety Group
- E-Safety Governor / Governors group
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Managing the Internet use in lessons:

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile Internet technology
- Staff will preview any recommended sites before use. Raw image searches are discouraged when working with students
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use Guidance for Staff:

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Don’t reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog.
- On-line gambling or gaming is not allowed.
- It is at the Headteacher’s discretion on what Internet activities are permissible for staff and students and how this is disseminated.

The use of removable Media:

Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school’s responsibility nor the network manager’s to install or maintain virus protection on personal systems.

If there are any issues related to viruses or anti-virus software, the network manager should be informed via e-mail.
Managing Other Web 2.0 Technologies Policy

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school / academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- At present, the school endeavors to deny access to social networking sites to students within school unless they are deemed educationally relevant (i.e. Pintrest and Twitter)

- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

- Students are taught to avoid placing images of themselves (or details within images that could give background details including for example school uniform) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

- Students are encouraged to be wary about publishing specific and detailed private thoughts online.

- Our students are asked to report any incidents of bullying to the school.

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the Moodle or other systems approved by the Headteacher. (see Twitter Policy for additional details)

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

**School staff should ensure that:**

- No reference should be made on personal social media accounts about students / pupils, parents / carers or school staff in the context of school related business.

- Personal opinions should not be attributed to the school /academy or local authority

- The school’s use of social media for professional purposes will be checked regularly by
the senior risk officer and e-safety group to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Other advice for staff:

- It is a good idea to keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online it is much easier to deal with this as soon as it appears. The UK Safer Internet Centres Reputation mini site has more information on this.
- Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
- Consider your own conduct online; certain behaviour could breach your employment code of conduct.
- Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.
- Do not accept friend requests from present pupils. You are also strongly advised not to accept requests to ‘friend’ or ‘follow’ from past students. Be aware that your social media friends may also be friends with current pupils and their family members and therefore could read your post if you do not have appropriate privacy settings.
- Do not give out personal contact details – if pupils need to contact you with regard to homework or exams, always use your school’s contact details. On school trips, staff should have a school mobile phone rather than having to rely on their own.
- Use your school email address for school business and personal email address for your private life; do not mix the two. This includes file sharing sites; for example Dropbox and YouTube.

If you are bullied online:

- You should never respond or retaliate to cyberbullying incidents. You should report incidents appropriately and seek support from your line manager or a senior member of staff.
- Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.
- Where the perpetrator is known to be a current pupil or colleague, the majority of cases can be dealt with most effectively through the school’s own mediation and disciplinary procedures.
- Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately. They can request that the person removes the offending comments.
- If they refuse either the school or you could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies for example, The UK Safer Internet Centre.
- If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the school may consider contacting the local police. Online harassment is a crime.
- Employers have a duty to support staff and no-one should feel victimised in the workplace. Staff should seek support from the senior management team, and their union representative if they are a member.
- The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the e-safety
issues which staff face, such as protecting professional identity, online harassment, or problems affecting young people; for example cyberbullying or sexting issues.

- The Safer Internet Centre has developed strategic partnerships with the key players in the internet industry. When appropriate, this enables the Professional helpline to seek resolution directly with the policy and safety teams at Facebook, Twitter, YouTube, Google, Tumblr, Ask.FM, Rate My Teacher and more.

Taken from (Further advice including links is contained within this document):


All members of the school community including staff, parents and students should ensure that:

- They do not engage in online discussion on personal matters relating to members of the school community.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
Parental Involvement Policy

We believe that it is essential for parents/carers to be fully involved with promoting E-Safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss E-Safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers and students are actively encouraged to contribute to adjustments or reviews of the school E-Safety policy by taking part in safety policy creation, giving review of the policy’s impact.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website).

- Parents/carers are expected to sign a Home School agreement containing the following statement or similar.

  “We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community”

- The school disseminates information to parents relating to E-Safety where appropriate in the form of;
  - Information and celebration evenings
  - Posters
  - Website/Learning Platform postings
  - Newsletter items
  - Learning platform training
Passwords and Password Security Policy

Passwords:

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Passwords must contain a minimum of six characters and be difficult to guess
- User ID and passwords for staff and students who have left the School are removed from the system within one month

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

Password Security:

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username.
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Staff will be required to change their password once a year. This will be of sufficient complexity to be safe. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is 60 min, however screens will lock after 10 min of inactivity.
- In our school, all ICT password policies are the responsibility of E-Safety Co-ordinator and all staff and students are expected to comply with the policies at all times

Zombie Accounts:
Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school’s systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorised access
- Regularly change generic passwords to avoid unauthorised access (Microsoft© advise every 42 days)

Further advice available [http://www.itgovernance.co.uk/](http://www.itgovernance.co.uk/)
Personal Information Promise

The personal information promise is:

I the Headteacher, on behalf of Saffron Walden County High School promise that we will:

1. value the personal information entrusted to us and make sure we respect that trust;

2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;

3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;

4. be open with individuals about how we use their information and who we give it to;

5. make it easy for individuals to access and correct their personal information;

6. keep personal information to the minimum necessary and delete it when we no longer need it;

7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;

8. provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don’t look after personal information properly;

9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and

10. regularly check that we are living up to our promises and report on how we are doing

More information available -


To view the promise

To sign up to the Promise

http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/personal_information.promise.aspx  go down to the bottom of the page
Personal or Sensitive Information Policy

Protecting Personal, Sensitive, Confidential and Classified Information:

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the Internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information:

- Using Removable Media Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean
Remote Access Policy

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to School systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment
Safe Use of Images and Video Policy

NB Please also see Star Lesson Appendix

Taking of Images and Film:

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images and video by staff and students with school equipment.

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school’s network and deleted from the staff device.

- Field trip advice. Students should be encouraged not to take or share images of others without their permission. At the parents information evening this should be shared with parents and the legal consequences of sharing inappropriate images should be discussed. A clause should also go into the letter to parents stating:

  "Images and Social Media

  We take E-safety very seriously and must ensure that we protect our students whilst they are in our care. Though it is fine for your child to take appropriate images of themselves and other students whilst on this trip, they should only do so with the permission of the others, this also applies to sharing images online. Please discuss the implications and consequences of taking and sharing inappropriate images with your child. Further information can be found on the school’s website and in the Acceptable Use Agreement."

As part of trip planning, the teacher in charge should check the image permission of the students going on the trip. If permission has not been given, no images of the student involved should be taken even by fellow students. This should be made clear before the trip commences.

Publishing Student’s Images and Work:

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school’s Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school’s communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child’s circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Students’ names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students’ full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Web Manager has authority to upload to the site.

Further information relating to issues associated with School websites and the safe use of images in Essex schools on the Essex Schools Infolink http://esi.essexcc.gov.uk

Storage of Images:

- Images/ films of children are stored on the school’s network and on Star Lesson Server
- Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform
- The Network Manager has the responsibility of deleting the images when they are no longer required, or the student has left the school

Webcams and CCTV:

- The school uses CCTV for security and safety. The only people with access to this are SLT and the Site Team Manager. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance: http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx
- We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes, i.e. approved Skype activity
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ‘inappropriate materials’ section of this document)
  - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images

For further information relating to webcams http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/Anti_Bullying/antibullying_cyberbullying_DCSF_sept07.pdf

Video Conferencing:

- Permission is sought from parents and carers if their children are involved in video
conferences

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All students are supervised by a member of staff when video conferencing
- All students are supervised by a member of staff when video conferencing with end-points beyond the school
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

For further information relating to Video Conferencing
https://www.education.gov.uk/publications/standard/_arc_Subjects/Page11/15007
School ICT Equipment including Portable & Mobile ICT Equipment

As a user of ICT, you are responsible for any activity undertaken on the school’s ICT equipment provided to you:

- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school’s inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school’s network drive. You are responsible for the backup and restoration of any of your data that is not held on the school’s network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
  - maintaining control of the allocation and transfer within their Unit
  - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment:

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy
• Staff must ensure that all school data is stored on school’s network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.

• Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

• Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.

• Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

• The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.

• In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

• Portable equipment must be transported in its protective case if supplied.

• Laptops and other school equipment should not be taken out of the country.

Mobile Technologies:

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible Internet access and thus open up risk and misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones and wearable technology such as the iWatch):

• The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/carer using their personal device.

• Sixth form students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent.

• This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer. Departments wishing to use a student’s personal device in years 7-11 should first read the policy in appendix 8.

• The school is not responsible for the loss, damage or theft of any personal mobile device.
• The sending of inappropriate text messages between any member of the school community is not allowed

• Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

• Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones and tablets):

• The sending of inappropriate text messages between any member of the school community is not allowed

• Permission must be sought before any image or sound recordings are made on the devices of any member of the school community

• Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used

• Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Removable Media:

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section ‘Error! Reference source not found.’.

• Only use recommended removable media

• Store all removable media securely

• Removable media must be disposed of securely by your ICT support team
Servers Policy

- Newly installed servers holding personal data should be encrypted, therefore password protecting data. SIMs Database Servers installed by SITSS since April 2009 are supplied with encryption software
- Always keep servers in a locked and secure environment
- Limit access rights to ensure the integrity of the standard build
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine’s specification
- Back up tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Back up tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Remote back ups should be automatically securely encrypted.
- Regular updates of anti-virus and anti-spyware should be applied
- Records should be kept of when and which patches have been applied
- Ensure that web browsers and other web based applications are operated at a minimum of 128 BIT cipher strength
Smile and Stay Safe Poster

E-Safety guidelines to be displayed throughout the school

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location).

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a ‘friend’.

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.
Systems and Access Policy

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses

- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or ECC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school’s business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

- It is essential that any hard drives which may have held personal or confidential data are ‘scrubbed’ in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing of the data.
Telephone Services Policy

- You may make or receive personal telephone calls provided:
  1. They are infrequent, kept as brief as possible and do not cause annoyance to others
  2. They are not for profit or to premium rate services
  3. They conform to this and other relevant ECC and school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

- Ensure that your incoming telephone calls can be handled at all times

- Follow the appropriate procedures in the event of receiving a telephone call containing office. If you do not have a copy, please ask your unit manager

School Provided Mobile Phones:

- You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles)

- Report the loss or theft of any school mobile phone equipment immediately

- The school remains responsible for all call costs until the phone is reported lost or stolen

- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it

- School SIM cards must only be used in school provided mobile phones

- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default

- You must not send text messages to premium rate services

- In accordance with the Finance policy on the private use of School provided mobiles, you must reimburse the school for the cost of any personal use of your school mobile phone. This includes call charges incurred for incoming calls whilst abroad. [To assist you in identifying personal use, add * to the end of the number being contacted, these will be shown separately on your bill]. Payment arrangements should be made through your finance administrator

- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.
Current Legislation

It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

The Act states that person data must be:
- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.


The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false

http://www.hmso.gov.uk/si/si2000/20002699.htm


Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
• Demonstrate standards, which are or ought to be achieved by persons using the system;

• Investigate or detect unauthorised use of the communications system;

• Prevent or detect crime or in the interests of national security;

• Ensure the effective operation of the system.

• Monitoring but not recording is also permissible in order to:

• Ascertain whether the communication is business or personal;

• Protect or support help line staff.

The school reserves the right to monitor its systems and communications in line with its rights under this act.


Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

• The right to a fair trial

• The right to respect for private and family life, home and correspondence

• Freedom of thought, conscience and religion

• Freedom of expression

• Freedom of assembly

• Prohibition of discrimination

• The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.


Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith; or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

http://www.legislation.gov.uk/ukpga/2006/1/contents

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child
under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of “Children & Families: Safer from Sexual Crime” document as part of their child protection packs.


For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.


The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual’s motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.


Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.


Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone’s work without obtaining them author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.
Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.


Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

The Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Appendix 1: Acceptable Use Agreement: Student - Secondary

Secondary Student Acceptable Use - Agreement / E-Safety Rules

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of the risks when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, Internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices/ wearable technology etc.) in school if I have permission or in the Sixth Form as set out in the BYOD policy. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however
this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings however trivial.
- I will only use social media sites with permission and at the times that are allowed.

**When using the Internet for research or recreation, I recognise that:**

- I should ensure that I have permission to use the original work of others in my own work. Where I do use the work of others, I should cite the author for reference.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the Internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

**In addition:**

- I understand that I am responsible for my actions, both in and out of school.
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / Internet, detentions, suspensions, contact with parents and in the event of illegal activities, involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.
Dear Parent/ Carer,

ICT including the Internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of E-Safety and know how to stay safe when using any ICT.

This form relates to the student Acceptable Use Agreement, to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Students are also expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their form teacher or the SWCHS E-Safety Co-ordinator.

Students: by signing you agree to follow these guidelines when:

- Using the school systems and devices (both in and out of school).
- Using your own devices in the school (when allowed) e.g. mobile phones, wearable technology, USB devices, cameras etc.
- I use my own equipment out of the school / academy in a way that is related to me being a member of this school / academy e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Parents: by signing this agreement you also agree to:

- Support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community

This Acceptable Use Agreement is a summary of our E-Safety Policy which is available in full via our publications scheme on our website.

Please return this form to school for filing via your child’s form tutor.

Student and Parent/ carer signature

We have discussed this document and ..............................................................(Student name) agrees to follow the E-Safety rules and to support the safe and responsible use of ICT at Saffron Walden County High School.

Parent/ Carer Signature .................................................................

Student Signature.................................................................

Form ........................................... Date ...........................................
Appendix 2: Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with The Director of ICT, SWCH school E-Safety Co-ordinator or Jennifer Sims, Safeguarding Officer. This Acceptable Use Agreement (for all staff, governors, visitors and students) is inclusive of both fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

✓ I will only use the school’s email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed ‘reasonable’ by the Head or Governing Body.
✓ I will comply with the ICT system security and not disclose any passwords provided to me by the school.
✓ I will ensure that all electronic communications with students and staff are compatible with my professional role (see staff conduct policy for guidelines).
✓ I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to students.
✓ I will only use the approved, secure e-mail system(s) for any school business.
✓ I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
✓ I will not install any hardware of software without permission of The Network Manager.
✓ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
✓ Images and video of students and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher. (See also Star appendix of E-Safety Policy)
✓ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
✓ I will respect copyright and intellectual property rights.
✓ I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
✓ I will support and promote the school’s E-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
✓ I understand this forms part of the terms and conditions set out in my contract of employment.

This Acceptable Use Agreement is a summary of our E-Safety Policy which is available in full via our publications scheme on our website.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ................................. Date .........................
Full Name ...........................................................................................................(printed)
Job title ..........................................................
Appendix 3: Curriculum E-Safety

Computing:

- In year 7 the students are taught in term 3 what to do in case of inappropriate conduct with people online or suspicious activity. The main guidelines from the thinkuknow website will be covered for that age range. The dangers of things being in the public domain and giving out content that is personal, cyber bullying, e stalking. They will be creating an informative video on the topic for a younger audience.

- They will also be told about CEOP and shown how to fill in the form on their website.

- Later in year 8 they will cover the laws associated with the use of computers within the UK.

- Throughout all Computing courses, students are taught how to search for relevant information on the web and are also taught the importance of ensuring that they do not plagiarise or breech copy write laws.

- UK laws with regard to Computing are revisited in most year groups for those who take opt to study Computing as a GCSE or A level subject.
Appendix 4: Use of Star Lesson Video Equipment

Protocols: Filming of lessons

It is important that all members of staff follow the protocols listed below as, of course, we have a duty to safeguard our students. If you have any questions or concerns regarding any of the following points, please see Christina Turner.

1. The member of staff who is recording the film is responsible for this film. They must follow these protocols. The member of staff may decide to share their film with another colleague but that will be their choice.

2. Members of staff must check the list of students who cannot be filmed before using the STAR filming app or stand-alone camera. I will send this via e-mail and save it in a folder on Public called STAR. If there are students in your class on this list, you can still film your lesson as long as the student who cannot be filmed is never visible on the recording.

3. Members of staff are able to film students within the school site if they do not appear on the list (e.g. in PE lessons, in classrooms, in groups etc.).

4. If the students are not on this list, members of staff are also able to film students on a school trip using an IPhone, Ipod or Ipad. This film cannot be viewed on this device and instead, will be saved onto the star lesson server. It can then be viewed on return to school and in school only. The film cannot be shared publicly and can only be shared in school.

5. Students from other schools cannot be filmed. This means that we cannot film sporting fixtures with other schools or any other event where children from other schools are involved. The only exception to this is the filming of students in our primary feeder schools and if this is to be undertaken, then you must speak to Polly Lankester in the first instance. She will then make the request with the primary school and ensure that no children who cannot be filmed are involved.

6. With permission from the class teacher, it is possible to film the lesson that this teacher is delivering or film students working within this lesson.

7. It is possible to export the film made so that it can be edited. However, you must let Christina Turner know if you want to do this so that editing permissions can be given. If it is exported, it must only be saved on the school network. It must not be shared outside of this school. Under no circumstances must it be uploaded to social media or YouTube. It may be uploaded onto Moodle for student access if the clip is of the teacher giving an explanation. It may be used for CPD purposes within SWCHS only.

8. The star lesson filming equipment/app can be used to observe the appraisal lesson but only with the permission of the teacher who is being appraised.
Appendix 5: BYOD Policy – Sixth Form

**Purpose:** For some time now students in the sixth form have been using their devices in school and connecting to the school network. This purpose of this policy is to clearly document our schools policy for BYOD in the sixth form, and formalise the use of the school network by individuals.

**Audience:** All students that access the school’s Wi-Fi networks, and/or use electronic devices to complete school work or self-directed learning or recreational activities while in school.

**Definition:** BYOD, an acronym for Bring Your Own Device, refers to any student-owned electronic device used to complete coursework, classwork, and other work in the process of learning a curriculum subject in a given content area.

**What You Can Use:** A device is prohibited if it is or otherwise potentially hazardous to the health of users, staff, or students. This means laptops, Android phones, iPhones, iPads, Google Tablets, Windows Phones, and other smartphones and tablets are approved if they allow you to complete your work without burdening school resources (see consequences), or the academic performance of your peers. Please note, you may only charge devices using approved chargers supplied by the manufacturer. No other alternatives can be permitted on the school premises.

**When in Doubt, Ask:** If you are unsure about whether a device is permitted in a lesson ask your teacher right away and ask if you’re unsure about a resource, network, app, or any related device use. We want you to benefit academically from the use of your device without damaging your device, or getting yourself in trouble. When in doubt, ask.

**Viruses & Malware:** Device security is the responsibility of the owner. Any device that threatens security of your device, or the software and hardware around you needs to be turned off and/or otherwise corrected.

**Other Risks:** Device theft, password security, damage from environment hazards and dropping, and interference from nearby devices are your responsibility to prevent, recognise, and/or correct. SWCHS network support department is not responsible for maintaining or troubleshooting your devices. The school does not provide insurance for your device, you bring it on to school grounds at your own risk.

**Connection:** All students will use the provided SSID and password to gain access to the wireless network and the Internet. The school does not guarantee connectivity or the quality of the connection.

**Digital Citizenship:** One definition of digital citizenship is “the self-monitored habits that sustain and improve the digital communities you enjoy or depend on.” Keep this in mind every time you send a text, update a social media profile, share a selfie, or recommend a resource to a friend, at school or at home. Your digital actions and behaviour are not only permanent, but deeply impact those around you, even if it’s not always immediately apparent how.
Think about how the use of your device might impact on a classroom environment. Approved devices must be in silent mode while in school unless otherwise allowed by a teacher. Headphones may be used only with a teacher’s permission. You must not have your device out outside of the sixth form area including the front of school and school corridors.

Devices may not be used to cheat on classwork, coursework, or tests or for non-instructional purposes (such as making personal phone calls and text messaging). You may not use devices to record, transmit, or post photographic images or video of a person or persons in school during school hours or during school activities, unless otherwise explicitly allowed by a teacher.

Devices may only be used to access computer files on Internet sites which are relevant to the classroom curriculum (see consequences).

Training: Training is not provided for use of individual devices, apps, or platforms. One of the goals of BYOD is for you to use a device that you’re comfortable with and accustomed to using under a variety of circumstances.

Bad Decisions: Any device use outside of the documented curriculum goals of a given classroom is prohibited, and in some cases punishable by law. Disrespectful communication, cyberbullying, spamming, sexting, copyright infringement, trolling, circumventing school filters or related device monitoring, and other abuses of technology will be documented, possibly leading to the loss of BYOD privileges, and enforcement by relevant law agencies.

This document does not replace the User Agreement for Electronic Equipment and Internet Use that your parents consented to, and signed on your behalf when you joined SWCHS. Please ensure you are familiar with the terms in the agreement. If you would like a copy, please contact The Director of ICT.

Consequences: You have a choice to follow the above guidelines, or to not follow the above guidelines. You have the choice to make good decisions, or not, to find “holes” in our policy or not, and to demonstrate digital citizenship or not.

- Should you choose to misuse your device in a lesson environment, a teacher has the right to revoke your permission to use it in a classroom.

- Bandwidth is an important resource to all members of our school community and should be used for learning purposes only. Should you choose to abuse your access to the schools network connection, you will have your bandwidth restricted, or in extreme cases access to the network will be blocked for your device. For example, you should not be streaming media for non-academic purposes (YouTube, NetFlix, Spotify).

- In the event of this happening any attempt to ‘get round’ restrictions (such as changing the MAC address on your device) will be considered a serious breach of trust that will require the involvement of the Director of Sixth Form.
Contact: The Director of ICT

Publication of Policy: This policy will be posted publicly at the school, shared on the school website, and supplied on request.
Appendix 6: SWCHS Twitter Guidance for Students

Principles

1. Use of Twitter is for the broadcasting of:
   a. educational resources
   b. information relevant to your academic career at SWCHS

2. Use of the SWCHS Twitter accounts is a teaching & learning activity and when using them you should at all times conduct yourself as though you were in school

Following a school Twitter account

1. All school account names will have “SWCHS” at the start (e.g. SWCHSMaths)

2. If unsure of the relevant account, ask your subject teacher to locate it for you

Specific Use

1. Once you have your own Twitter account, you are able to ‘follow’ any school Twitter account

2. Searching for ‘hashtagged’ conversations is a good way of finding specific Tweets that are relevant to you. Your teacher will let you know which hashtags they are using

3. Do not send direct messages to your teachers via Twitter. You should use your school email account or speak to them in person

4. Your account is your responsibility. Teachers will not browse, follow or tweet directly to your individual accounts, but you should still think carefully about what you tweet and what impression you give to other people using Twitter

If you are concerned about anything you see or receive on Twitter, please speak to your tutor or to any member of staff
Appendix 7: SWCHS Twitter Guidance for Staff

Principles:

- Use of Twitter is for the broadcasting of:
  - educational resources
  - information relevant to students’ academic career at SWCHS
- Use of Twitter is a teaching & learning activity and as such will be conducted solely in the manner befitting a professional student-teacher relationship
- Twitter is for use with students aged 13 & over, therefore accounts can only be used in Years 9-13.

Accounts:

- All account names are to be prefaced with “SWCHS” (e.g. SWCHSMaths)
- All login details are to be sent to ICT Support to be kept in a central register
- Each Twitter Account MUST be monitored by more than one member of staff

Specific Use:

- Tweets are to be open broadcasts, available to be followed by anyone.
- Tweets may be tagged in order to differentiate the target audience
- Staff are not permitted to browse, follow or tweet to students’ Twitter accounts
- Staff are not permitted to follow the school Twitter feeds using their own personal Twitter account
- Direct messaging between staff and students is not permitted
- Tweets are to be appropriate for classroom use and as such conform to school policies and procedures
- Before sending a tweet, staff accept responsibility for checking the content of the tweets (including links and retweets) for appropriate language and content
Appendix 8: BYOD Policy Years 7-11

Current school rules state that students in year 7-11 are not permitted to bring a mobile phone, tablet or other device to school.

However, in approved circumstances that are proven to be educationally beneficial staff can follow the following policy:

1. Seek approval for the proposed activity from AC and put request in writing to E-Safety Co-ordinator including a draft of parental letter. Await approval.
2. Seek written permission from parents using the letter template below.
3. Plan activity carefully with due consideration to the e-safety policy guidance.

Dear Parent/Carer,

(Introductory paragraph including activity and rationale)

I am therefore asking for your permission to allow (name) to bring in a device for the specific purpose mentioned above. (Name) should still adhere to the normal rules regarding mobile devices in all other lessons and when on the school site.

Please be aware that by giving your permission you are agreeing to the rules set out in the Sixth Form BYOD policy on use (available on school website and within school safety policy). In particular:

“Device theft, password security, damage from environment hazards and dropping, and interference from nearby devices are the student’s responsibility to prevent, recognise, and/or correct. SWCHS network support department is not responsible for maintaining or troubleshooting student’s devices. The school does not provide insurance for student’s personal devices, they bring them on to school grounds at their own risk.”

Student’s are required to access the Internet through the school provided SSID only. Mobile data should be switched off on any device whilst it is being used for the activity. This is to ensure that students are subject to normal filtering of explicit and inappropriate content.

(closing paragraph including your contact details).
Appendix 9: E-Safety Group Terms of Reference

Purpose:

To provide a consultative group that has wide representation from the school and community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Full Governing Body.

Membership:

The e-safety group will seek to include representation from all stakeholders.

The composition of the group should include:

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- E-safety coordinator (not ICT coordinator by default)
- ICT Technical Support staff
- Community users (where appropriate)
- Digital Leaders (Student / pupil representation – for advice and feedback. Student / pupil voice is essential in the make up of the e-safety group, but students / pupils would only be expected to take part in group meetings where deemed relevant.)

Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the group to provide advice and assistance where necessary.

Group members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

Group members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

Chairperson:

The Group should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying group members;
- Inviting other people to attend meetings when required by the group;
• Guiding the meeting according to the agenda and time available;
• Ensuring all discussion items end with a decision, action or definite outcome;
• Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

**Duration of meetings:**
Meetings shall be held termly for a period of no more than one hour. A special or extraordinary meeting may be called when and if deemed necessary.

**Functions:**
These are to assist the E-safety Co-ordinator (or other relevant person) with the following:

• To keep up to date with new developments in the area of e-safety
• To (at least) annually review and develop the e-safety policy in line with new technologies and incidents
• To monitor the delivery and impact of the e-safety policy
• To monitor the log of reported e-safety incidents (anonymous) to inform future areas of teaching / learning / training.

To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-safety. This could be carried out through:

• Staff meetings
• Student / pupil forums (for advice and feedback)
• Governors meetings
• Surveys/questionnaires for students / pupils, parents / carers and staff
• Parents evenings
• Website/VLE/Newsletters
• E-safety events
• Internet Safety Day (annually held on the second Tuesday in February)
• Other methods
• To ensure that monitoring is carried out of Internet sites used across the school
• To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
• To monitor the safe use of data across the [school]
• To monitor incidents involving cyberbullying for staff and pupils

**Amendments:**
The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all group members, by agreement of the majority.
Appendix 10 : Further Reading

**UK Safer Internet Centre:**
Safer Internet Centre -
South West Grid for Learning
Childnet
Professionals Online Safety Helpline
Internet Watch Foundation

**CEOP:**
http://ceop.police.uk/       ThinkUKnow

**Others:**
UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis
Netsmartz  http://www.netsmartz.org/index.aspx

**Support for Schools:**
Specialist help and support   SWGfL BOOST

**Cyberbullying:**
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government  Better relationships, better learning, better behaviour
DCSF - Cyberbullying guidance
DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies
Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
Cyberbullying.org - http://www.cyberbullying.org/

**Social Networking:**
Digizen – Social Networking
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connectsafely Parents Guide to Facebook
Facebook Guide for Educators

**Curriculum:**
SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Alberta, Canada - digital citizenship policy development guide.pdf

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Somerset - e-Sense materials for schools

Mobile Devices / BYOD:

Cloudlearn Report  Effective practice for schools moving to end locking and blocking

NEN  - Guidance Note - BYOD

Data Protection:

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

ICO pages for young people

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List
Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

**Professional Standards / Staff Training:**

DfE - Safer Working Practice for Adults who Work with Children and Young People

Kent - Safer Practice with Technology

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

**Infrastructure / Technical Support:**

NEN - Guidance Note - esecurity

**Working with parents and carers:**

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

Connect Safely - a Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

DirectGov - Internet Safety for parents

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

The Cybersmile Foundation (cyberbullying) - advice for parents

**Research:**

Appendix 11: Forms and Templates

Record of reviewing devices / Internet sites (responding to incidents of misuse):

<table>
<thead>
<tr>
<th>Group</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>Reason for investigation</td>
<td></td>
</tr>
</tbody>
</table>

Details of first reviewing person

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

Details of second reviewing person

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

Name and location of computer used for review (for web sites):

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

Web site(s) address / device:  

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>

Reason for concern:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>

Conclusion and Action proposed or taken:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Reported by</td>
<td>Signature</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Training Needs Audit:

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Review date</th>
<th>To be met by:</th>
<th>Identified training need</th>
<th>Relevant training in last 12 months</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>