SOUTHBOROUGH
HIGH SCHOOL

SOUTHBOROUGH HIGH SCHOOL eSAFETY AND DATA PROTECTION POLICY

PHILOSOPHY

ICT in the 21st Century is seen as 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

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

PURPOSE

- At Southborough High School we understand the responsibility to educate our pupils on eSafety 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 pupils) 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 pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

PRACTICE

- **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.

- **Breaches**

    - A breach or suspected breach of policy by a School employee, contractor or pupil 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.
    - Policy breaches may also lead to criminal or civil proceedings.
    - The ICO's new powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices

requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

- The data protection powers of the Information Commissioner's Office are to:
    a. Conduct assessments to check organisations are complying with the Act;
    b. Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
    c. Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
    d. Prosecute those who commit criminal offences under the Act;
    e. Conduct audits to assess whether organisations processing of personal data follows good practice,
    f. Report to Parliament on data protection issues of concern

✶ 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 SIRO or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner.
- Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

✶ Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD) are automatically checked for any viruses using school provided anti-virus software
- Never interfere with any anti-virus software installed on school ICT equipment that you use
- 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

✶ Data Security

- The accessing and appropriate use of school data is something that the school takes seriously.
- The school follows Becta guidelines Becta Schools - Leadership and management - Security - Data handling security guidance for schools (published Spring 2009) and the Local Authority guidance documents listed

below

- Headteacher’s Guidance – Data Security in Schools – Dos and Don’ts
- Network Manager/MIS Administrator or Manager Guidance – Data Security in Schools
- Staff Guidance – Data Security in Schools – Dos and Don’ts
- SIRO/IAO Guidance – Data Security in Schools - Dos and Don'ts
- The Head, SIRO and Network Manager documents contain advice about identifying information assets including an example of an excel spreadsheet and a brief outline of the school policy that can be displayed at appropriate sites within the school or handed to visitors or guests.

✶ Security

- The School gives relevant staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff have read the relevant guidance documents available on the SITSS website concerning ‘Safe Handling of Data’
- Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO)
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used
- Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent.

✶ Impact Levels and Protective Marking

- Appropriate labelling of data should help schools secure data and so reduce the risk of security incidents
- Apply labelling in accordance with guidance from your Senior Information Risk Owner (SIRO)
- Most learner or staff personal data will be classed as Protect
- Protect and caveat classifications that schools may use are;

  PROTECT – PERSONAL e.g. personal information about an individual
  PROTECT – APPOINTMENTS e.g. to be used for information about visits from the Queen or government ministers
  PROTECT – LOCSEN e.g. for local sensitive information
  PROTECT – STAFF e.g. Organisational staff only

RESTRICTED – STAFF e.g. A large amount of data (information on over 20 persons)

RESTRICTED – PUPILS e.g. A large amount of data (information on 20 persons)

- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents
- Reviews are continuing to look at the practical issues involved in applying protective markings to electronic and paper records and government representatives are working with suppliers to find ways of automatically marking reports and printouts.

✶ **Senior Information Risk Owner (SIRO)**

The SIRO is a senior member of staff who is familiar with information risks and the school's response. He has the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

✶ **Information Asset Owner (IAO)**

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Please refer to the appendix at the back of this document showing examples of information assets a school may hold.

The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc including UPN, teacher DCSF number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

✶ **Disposal of Redundant ICT Equipment Policy**

All redundant ICT equipment will be disposed off through an authorised agency or via the Kingston upon Thames disposal scheme. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this

will happen
Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The school's disposal record will include:
  - Date item disposed of
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? *
  - How it was disposed of eg waste, gift, sale
  - Name of person & / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

- **Waste Electrical and Electronic Equipment (WEEE) Regulations**
- **Environment Agency web site**

✶ **e-Mail**

- The use of e-mail within most schools is an essential means of communication for both staff and pupils. 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 pupil based, within school or international.
- We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette;'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving e-mails.

✶ **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 pupils, 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'. The responsibility for adding this disclaimer lies with the account holder

- 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 pupils are advised to cc. the Headteacher, line manager or designated account
- Pupils 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 pupil 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
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the ICT 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 Hotmail, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving e-mail is not permitted and blocked.

✶ **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

- e-mailing Personal, Sensitive, Confidential or Classified Information
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- If you are required to send an e-mail from someone else's account, always sign on through the 'Delegation' facility within your e-mail software so that you are identified as the sender (if available within your software)
- 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 2 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 Receiving e-Mails
- Check your e-mail regularly

- Activate your 'out-of-office' notification when away for extended periods
- Use the 'Delegation' facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)
- Never open attachments from an untrusted source; Consult your network manager first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

✶ 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 where possible
- The use of Hotmail, BTInternet, AOL or any other 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:
  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
  - 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)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

In exceptional circumstances, the Local Council makes provision for secure data transfers to specific external agencies.

✶ Future Developments

- There is currently a review taking place on the way e-mails are sent whereby all such communications are sent using GCSx.
- GCSx stands for the Government Connect Secure eXtranet. It provides a more secure communications system (i.e. more secure than the internet).
- When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a pupil, for example, you need to put in **PROTECT – PERSONAL** on the first line of the e-mail.

- This also needs to go on the top of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security

✶ Equal Opportunities - Pupils with Additional Needs

- The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.
- However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.
- Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

✶ eSafety - Roles and Responsibilities

- As eSafety is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.
- The eSafety co-ordinator has been designated this role as a member of the senior leadership team.
- All members of the school community have been made aware of who holds this post.
- It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as LA, CEOP (Child Exploitation and Online Protection) and Childnet.
- Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.
- This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

✶ eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in ICT/ PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils 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
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

✶ **eSafety Skills Development for Staff**

- Our staff receive regular information and training on eSafety issues in the form of training supplied by Kingston.
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

✶ **Managing the School eSafety Messages**

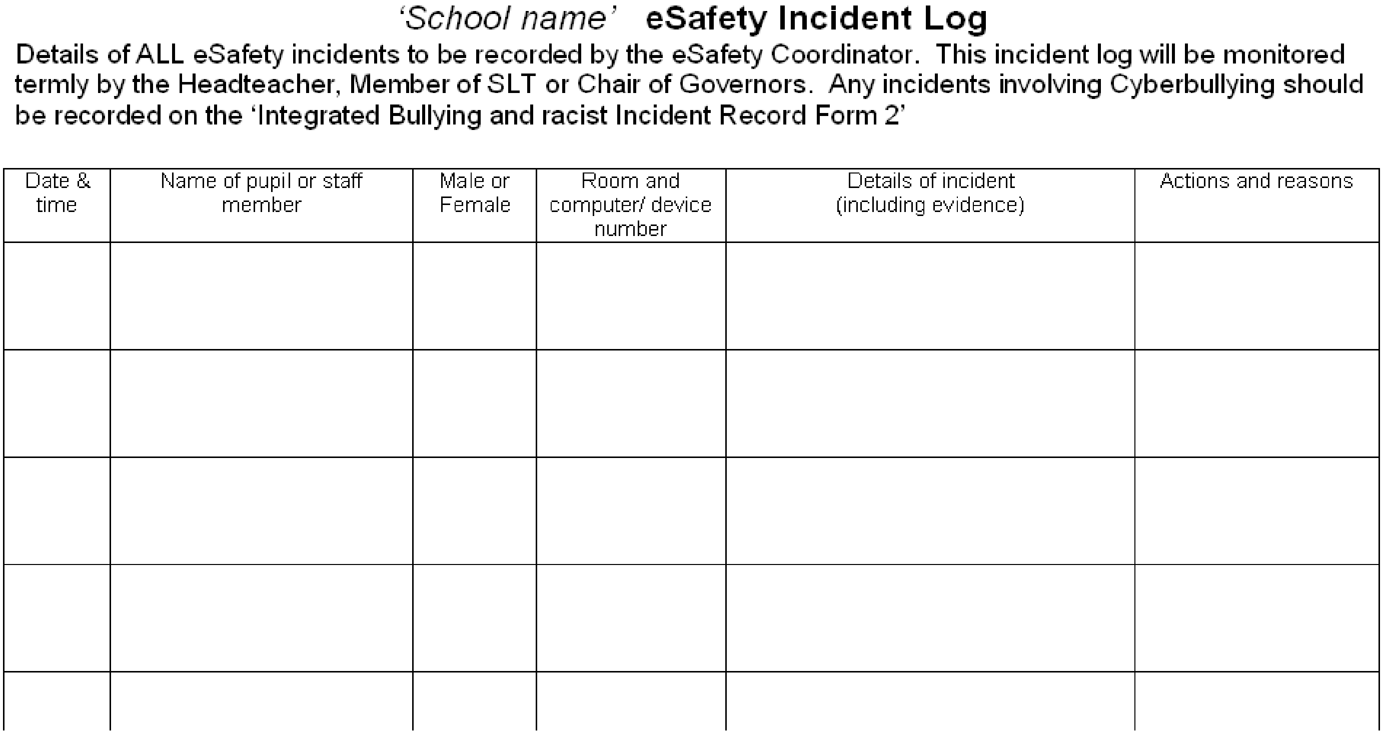
- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- The eSafety policy will be introduced to the pupils at the start of each school year
- eSafety posters will be prominently displayed

✶ **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 SIRO or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner.

✶ eSafety Incident Log

Some incidents may need to be recorded in other places, such as Solero, if they relate to a bullying or racist incident



‘School name’ **eSafety Incident Log**

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the ‘Integrated Bullying and racist Incident Record Form 2’

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

✶ Misuse and Infringements - Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher.

✶ Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety 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)
- Users are made aware of sanctions relating to the misuse or misconduct by ***accepting the Securus AUP each time they log on.***

✶ Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

✶ **Managing the Internet**

- 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 pupils
- 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**

- 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 pupils and how this is disseminated.

✶ **Infrastucture**

- School internet access is controlled through the LA's web filtering service.
- Southborough High Schoolemploys some additional web filtering which is the responsibility of ***the Information Systems Manager/Senior IT Technician.***
- Southborough High School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils 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
- Pupils 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 pupils wish to bring in work on removable media it must be given to the ***technician/teacher*** for a safety check first

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from ***the technician/ICT subject leader.***
- If there are any issues related to viruses or anti-virus software, the network manager should be informed in writing.

✶ Managing Other Web 2 Technologies

- 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 pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking sites to pupils within school
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils 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 pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- Our pupils 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 pupils using the LA Learning Platform or other systems approved by the Headteacher

✶ Parental Involvement

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

  - Information and celebration evenings
  - Posters
  - Website/ Learning Platform postings
  - Newsletter items
  - Learning platform training

✶ **Passwords**

- Pupils use theirr own personal passwords to access computer based services
- Pupils do not include passwords in any automated logon procedures
- Staff are instructed to change temporary passwords at first logon
- All users care instructed to change passwords whenever there is any indication of possible system or password compromise
- All users care told not to record passwords or encryption keys on paper or in an unprotected file
- Users are advised to disclose personal password only 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 pupils who have left the School are removed from the system automatically once removed from SIMS.

✶ **Password Security**

- Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils 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. From admission they are also expected to use a personal password and keep it private
- Pupils 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, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. 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 ***2 hours.***
- Due consideration should be given when logging into the Learning Platform to

the browser/cache options (shared or private computer)

- In the school, all ICT password policies are the responsibility of **Information Systems Manager/Senior Network Manager** and all staff and pupils are expected to comply with the policies at all times

✶ Protecting Personal, Sensitive, Confidential and Classified Information

All users are advised to:

- 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 a manager
- That one 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 any screen display out of direct view of any third parties when 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

✶ Removable Media

Users are advised to:

- 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

Users are advised to:

- Be responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- 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

✶ 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 pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, 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
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, 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 pupil's device

✶ Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

✶ Publishing Pupil'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, ie exhibition promoting the school
- general media appearances, eg 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, eg 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.
- ➢ Pupils' names will not be published alongside their image and vice versa.
- ➢ E-mail and postal addresses of pupils will not be published.
- ➢ Pupils' 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.

✶ <u>**Storage of Images**</u>

- Images/ films of children are stored on the school's system.
- Pupils 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 pupils within the confines of the school network/ Learning Platform
- ***Information Systems Manager/Network Manager*** has the responsibility of deleting the images when they are no longer required, or the pupil has left the school

✶ <u>**Webcams and CCTV**</u>

- The school uses CCTV for security and safety.
- We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes
- 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)

✶ <u>**Video Conferencing**</u>

- 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 pupils are supervised by a member of staff when video conferencing
- All pupils 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

✶ <u>**School ICT Equipment**</u>

- Users of ICT are responsible for any activity undertaken on the school's ICT equipment provided to you
- We log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Visitors are not to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to wireless ICT Facilities if available
- Users are asked to ensure that all ICT equipment is kept physically secure
- Users must 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
- Users are asked to ensure that data is saved on a frequent basis to the school's network drive. They are responsible for the backup and restoration of any 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
- A time locking screensaver is applied to all machines. Any PCs etc accessing personal data 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 the user's responsibility to ensure that any information accessed from a 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)

✶ <u>**Portable & Mobile ICT Equipment**</u>

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 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 the car before starting a 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

✶ **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)**

- 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 pupil or parent/carer using their personal device
- Pupils 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
- 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)**

- 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 ‘

Removable Media’

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

✶ Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- 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

✶ Smile and Stay Safe Poster

SMILE **and stay safe**

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 my 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

- Users are responsible for all activity on school systems carried out under any assigned access/account rights, whether accessed via school ICT equipment or a personal PC
- Unauthorised persons are not allowed to use school ICT facilities and services that have been provided.
- Users are to only use their own personal logons, account IDs and passwords and are not to allow them to be used by anyone else
- Users should keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information
- Users should lock their screen before moving away from theirr computer during normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Users should ensure that they logoff from the PC completely when going to be away from the computer for a longer period of time
- Users are not to introduce or propagate viruses
- It is imperative that a user does not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC 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, permission should be obtained from the owner or owning authority and payment made of 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 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 is appointed to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

✶ Telephone Services

- You may receive personal telephone calls provided they are infrequent, kept as brief as possible and do not cause annoyance to others
- 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 a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask your unit manager

POLICY REVIEW

This policy will be reviewed annually during the Summer Term.

Date: April 2018

Appendix 1

SOUTHBOROUGH HIGH SCHOOL STUDENT'S ACCEPTABLE USE POLICY for ELECTRONIC DEVICES

Use of Electronic Resources

A. Use of electronic resources including the internet, e-mail and other systems must be in support of the educational goals and policies of Southborough High School.

B. **Use of any electronic resource** must be consistent with the rules appropriate to the resource. This includes, but is not limited to, laws and regulations regarding:

a. Copyrighted material
b. Threatening, obscene or profane material
c. Material protected by trade secret
d. Sexual, racial, ethnic, or religious harassment
e. Privacy

C. Prohibited Activities:

a. Using another individual's username and password.
b. Using electronic resources for financial gain, for political activity, or personal business activity.
c. Accessing, downloading, storing, viewing, sending, or displaying text, images, movies, or sounds that contain pornography, obscenity, or language that offends or tends to degrade others.
d. Attempting to send, or sending, anonymous messages of any kind or pretending to be someone else while sending a message.
e. Attempting to, or actually accessing, modifying, harming or destroying another user's data.
f. Harassing, insulting, threatening, or attacking others via electronic resources.
g. Electronically or physically damaging or attempting to damage the network, equipment, materials or data.

i. Attempting to or actually accessing the School network or any devices attached to the

ii. network without authorization or in violation of any law. Examples include hacking, flooding or virus deployment.

i. Using telephone services, including long distance, without authorization.
j. Using electronic resources for illegal or inappropriate activities.

Electronic resources include but are not limited to

☐ Network access
☐ Internet access
☐Digital cameras
Personal digital assistants, *e.g.*, PDAs, Pocket PC, Palm OS devices
☐ Personal communication devices, *e.g.*, mobile phones, pagers, messaging devices, telephones

☐ mp3 players
☐ USB flash drives
☐ E-mail
☐ Computers
  ☐Laptops

k. Accessing confidential student or employee information without authorization or through misuse of authorization and communicating such information with unauthorized persons.
l. Other uses that the School may deem to be unacceptable.

Internet Safety
Southborough High School provides a variety of measures to ensure the safety of online activities of minors.
Included measures are:
a. Filtering and blocking access to inappropriate matter on the internet.
b. Active monitoring of online activities of students.
c. Procedures to prevent unauthorized disclosure, use and sharing of personal information regarding students.
d. Procedures on the use of electronic mail, chat rooms and other forms of direct electronic communication.

No Privacy
Users have no expectation of privacy in any communication sent or received by email, or in regard to the internet, network access, or other electronic resources, material stored on or using any school provided electronic device or material that is stored on any personal electronic device that is connected to the School network.

Privileges

The use of Southborough High School electronic resources is a privilege.
Inappropriate, prohibited, or unauthorized use may result in cancellation of a user's privilege and referral for appropriate disciplinary/legal action. Each individual user who is authorized for access will receive information pertaining to the proper use of the resources.
Administrators will decide if usage is inappropriate, prohibited, or unauthorized and their decision is final. The school may limit or terminate access at any time if deemed necessary. In addition, teachers are authorised to limit or terminate student class use.

Security Measures

User names, passwords and other measures are used to maximize security. Procedures are in place to notify appropriate personnel should a security problem be identified. These procedures include notification of teachers, staff and appropriate administrators.

Liabilities

Southborough High School makes no guarantees of any kind, whether expressed or implied, for the services provided. The school is not responsible for any damages suffered, including loss of data in conjunction with the use of its networks or equipment. In addition, the school is not responsible for the accuracy or quality of information or data obtained through the use of electronic resources.

Netiquette

Users are required to abide by the rules of communications etiquette. This includes being polite, abstaining from the use of vulgar or obscene language, and providing timely responses to communication.

Updating User Information

Users must notify their school's office of any changes in account information (address, school, or any other relevant data) in order to continue using electronic resources.

Acceptance of Terms and Conditions

All terms and conditions, as stated in this Acceptable Use Policy, are applicable to each user. By signing this document, you are accepting these terms and conditions. Without your signature, you will not be allowed access to the school's electronic resources.

Disciplinary Actions

If a student violates any of the areas of this policy, his/her access may be limited or terminated and future access may be denied. In addition, appropriate disciplinary actions may be taken including, but not limited to, suspension, expulsion, legal action and/or referral to law enforcement.

AUP Implementation Guidelines

Students are required to comply with the guidelines for implementation of this policy as published by Southborough High School.
The guidelines are an integral part of this policy.

Southborough High School reserves the right to change this policy at any time.

This section to be signed by the student.

In order that I may access the electronic resources, I agree to comply with the school's procedures and restrictions as detailed above.

I will use the network in a responsible way and observe all the restrictions explained to me by the school and in the Acceptable Use Policy.

I agree to report any misuse of the network to either an IT Technician or the Network Manager. If I do not follow the rules, I understand that this will result in loss of access to the network as well as other disciplinary action.

I understand that I will be barred from using the network if found to be abusing my privileges.

I have read and understood the AUP and agree to abide by it.

Pupil Name (*block capitals*):
____

Pupil Signature: _________________________________

Date: ______-______-______

This section to be read and signed by the parent/legal guardian of the above student.

As the parent/legal guardian of the pupil named above, I give permission for my son to access Southborough's electronic resources.

I accept responsibility for setting standards for my son to follow when selecting, sharing and exploring information and media. I agree to report any misuse of the network to the school.

I have read and understood the AUP and agree to ensure that my son abides by it.

Parent/Legal Guardian Name (*block capitals*):
____

Parent Signature: _________________________________

Date: ______-______-______

Acceptable Use Agreement: Pupils - Secondary

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/ Learning Platform with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes inline with school policy and not be distributed outside the school network without the permission of a senior teacher.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be

contacted.

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 pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of eSafety and know how to stay safe when using any ICT.

Pupils are 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 ICT class teacher or the school eSafety coordinator.

Please return the bottom section of this form to school for filing.

✂

Pupil and Parent/ carer signature

We have discussed this document and …………………………………..........(pupil name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at Southborough High School.

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

Pupil Signature…………………………………………………………….

Form ………………………………… Date ………………………………

Acceptable Use Agreement: Staff, Governors and Visitors

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 school eSafety coordinator or the Head of ICT

- 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 or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- 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 MIS software) 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 eSafety coordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline 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.
- 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 support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- 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 pupils 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.

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 ……………………………………………………………………………...