South End Junior School	**Page 1 of 14**
	Issued: 24 November 2016
On-Line Safety Policy	**Review date: When necessary or events change**
	Supersedes: 7 Sept 15
Approved by	~~FULL GOVERNING BODY~~/L & M COMMITTEE/~~HEADTEACHER~~

ON-LINE SAFETY POLICY

Introduction

The On-Line Safety Policy is related to other Policies including those for Computing, Bullying, Child Protection, Data Protection and Acceptable Use.

This policy has been written in compliance with the DCSF December 2009 'Guidance for safer working practices for adults working with children and young people in educational settings'.

This policy will be reviewed **when necessary** and consideration given to the implications for future whole school development planning. It will be amended earlier if new technologies are adopted or Central Government change the orders or guidance in any way

Rationale

Computing 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 computing within our society as a whole. Currently the internet technologies available both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Social Networks (Facebook, Twitter, Edmodo, etc.)
- 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
- Tablets (including iPads and Kindles)
- Webinars

Whilst exciting and beneficial both in and out of the context of education, much computing, 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 and that adults

and children are aware of their roles, responsibilities and procedure for the acceptable, safe and responsible use of all technology.

At South End Junior, we understand the responsibility to educate our students on On-Line Safety issues; teaching them the appropriate behaviours to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. All students from September 2015 will sign an acceptable usage policy that they agree to abide by when using SEJA technologies and internet. Parents will be sent home a copy of this document so they are made aware of safe procedures when using the above at home. Another copy of the signed document will be kept in each pupil's personnel file.

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. The school has a Data Protection Policy which should be referred to.

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 are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, 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).

Teaching and Learning

Why the Internet and digital communications are important

The internet is an essential element in 21st century life for education, business and for social interaction. South End Junior School has a duty to provide students with quality internet access as a part of their learning experiences.

Use of the internet is a part of the statutory curriculum and a necessary tool for students and staff. The school will ensure that there is secure web filtering to prevent access to undesirable websites. We liaise closely with our internet provider to ensure that our pupils are safe when using internet applications.

Internet use will enhance learning

The school internet access for student use will include filtering appropriate to the age of the students. Students will be taught what Internet use is acceptable and what is not. (See Online Rules – Appendix 3). The school will ensure that the use of Internet derived materials by students and staff complies with copyright law.

Managing 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.

The school has 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
- Pupils are prohibited from conducting raw image searches
- Pupils should not access the internet if unsupervised
- If Internet research is set for homework (if appropriate to individual students), 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

Information System Security

The School ICT systems security will be reviewed regularly, to ensure appropriate controls are in place with regard to access. Virus protection will be updated regularly. (See "Computer Viruses below)

E-Mail

Children do not have their own email accounts. If their computing scheme of work covers emailing then a platform will be arranged, ensuring security.

On-Line Safety Roles and Responsibilities

This policy, supported by the school's Acceptable Use Policy and Data Protection Policies is to protect the interests and safety of the whole school community.

Head and Governors

As On-Line Safety 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 named On-Line Safety co-ordinator in this school is Georgie Lewis and the On-Line Safety Governor is Margaret Barnes. All members of the school community will be made aware of who holds these posts.

Roles and responsibilities of On-Line Safety coordinator

- Recognise the importance of On-Line Safety and understand the school's duty of care for the On-Line Safety of their pupils and employees.

- Establish and maintain a safe computing learning environment within the school.

- Coordinator to provide CEOP materials for staff to share with pupils at the beginning of each year and to be referred to throughout the year.

- With the support of the IT Technician, ensure that filtering is set to the correct level for employees, young volunteers, children and young people accessing school equipment.

- Report issues of concern and update the Principal on a regular basis.

- Liaise with the Anti-Bullying, Child Protection and computing leads so that procedures are updated and communicated, and take into account any emerging On-Line Safety issues and technological changes.

- Co-ordinate and deliver employee training according to new and emerging technologies so that the correct On-Line Safety information is being delivered.

- Maintain an On-Line Safety Incident Log to be shared at agreed intervals with the Principal and Governors at governing body meetings. Log should be cross-referenced in a child concern form.

- With the support of the IT Technician, implement a system of monitoring employee and pupil use of school issued technologies and the internet where a concern has been raised.

- Host parent workshops to ensure the school's best internet safety practice is shared and reflected at home.

Misuse and Incident Reporting

Any security breaches or attempts, loss/stolen equipment and any unauthorised use of computing must be immediately reported to the school's On-Line Safety Coordinator and Business Manager and recorded on the appropriate documentation (appendix 1). Additionally, all security breaches, lost/stolen data, virus notifications, unsolicited emails, misuse or unauthorised use of computing and all other policy non-compliance must be reported to the On-Line Safety coordinator who will advise the Business Manager if the incident pertains to loss of personal data.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media must be checked for any viruses using school provided anti-virus software before using them. This should occur automatically when the device is introduced to the school system.
- Never interfere with any anti-virus software installed on school computing equipment that you use
- If your laptop is not routinely connected to the school network, you must be aware that virus protection may not be up-to-date. When you reconnect your machine to the school network and go onto the internet, the virus protection should automatically up-date.

  To check that virus protection is up-to-date or up-date virus protection right click on the virus protection tab and follow appropriate actions.
- If you suspect there may be a virus on any school computing equipment, stop using the equipment and contact your computing Team immediately. The computing Team will advise you what actions to take and be responsible for advising others that need to know

Monitoring

Authorised computing staff may inspect any computing equipment owned or leased by the School at any time without prior notice.

The School may monitor telephone, email and internet traffic data (i.e. sender, receiver, subject, date and time of text messages; non-business attachments to email; numbers called and duration of calls; domain names of web sites visited, duration of visits; and non-business files downloaded from the internet) at a network level (but covering both personal and

business communications) for the purposes outlined above. You need to be aware that such monitoring might reveal sensitive personal data about you. For example, if you visit web sites which detail the activities of a particular political party or religious group, then these visits might indicate your political opinions or religious beliefs. Computing 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.

Please note that personal communications using School computing may be unavoidably included in any business communications that are monitored, intercepted and/or recorded. Please see Data Protection Policy.

Passwords and 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 accept appropriate personnel.

- Users are provided with (if appropriate) an individual network, email, Learning Platform and Management Information System log-in username.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, systems and/or Learning Platform. Individual staff users must also make sure that workstations are logged off after use.
- Students have their own logins to their domains but are not permitted to change their login details.

Social Networking

Staff will have access to a copy of the "Guide for Professionals Working with Young People" – Using Social Networking Safely.

Staff using social networking sites should:-

- Ensure that privacy settings are set to maximum
- Be aware that behavior in their personal life may impact upon your work with children
- Think about changing their Facebook profile picture and username to keep prying eyes out. E.g. Use a cartoon image and a nickname.
- Seek advice from Principals or Vice Principal if they are contacted by pupils or ex-pupils under the age of 18

Staff using social networking sites should not:-

- Use or access social networking sites of pupils.
- Give their personal contact details to pupils, including their mobile telephone number/email.
- Rely on Facebook privacy settings entirely; they change frequently and still allow for

contacts to 'tag' or copy content from your profile, potentially sharing it with the wider world.

- Write comments or post pictures online that they would not show the Principals or colleagues. (Once something is posted on-line, control of it is lost completely).
- Not post any text, image, sound or video which could upset or offend any member of the whole school community or be incompatible with their professional role.
- List pupils as approved contacts
- Use or access social networking sites of pupils or ex-pupils under the age of 18 years unless they are a family member.
- Post photographs / pictures of school life/staff/pupils on the social networking site.

Safe Use of Images

Taking of Images an 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.

Publishing students images and work

South End Junior School seeks the consent of parents (on behalf of students) and staff, to use images and film for assessment and educational purposes including the inclusion of images on the school website and an up to date list is distributed to staff.

On entry to the school, all parents/carers will be asked to give permission to publish their child's/young person's photos in the newspaper or on our school internet site.

This consent form is considered valid for the entire period that the child/young person attends this school unless there is a change in the child's/young person'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.

Before posting anything on the Internet that identifies the person, a check needs to be made to ensure that permission has been given.

Storage of Images

- Images/ films of students are stored on the school's equipment
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform

School computing Equipment including Portable & Mobile computing Equipment & Removable Media

School computing Equipment

- As a user of computing, you are responsible for any activity undertaken on the school's computing equipment provided to you
- The school logs computing equipment issued to staff and records serial numbers as part of the school's inventory. Staff sign and accept the school's terms on issue of any equipment e.g. laptops, iPads.
- Ensure that all computing 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 wherever possible when leaving work stations unattended staff should log off or screen lock. As a minimum administration staff should set up a screensaver Workstations must be switched off at the end of each working day.
- On termination of employment, resignation or transfer, return all ICT equipment
- 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 (see Data Protection Policy)

Portable & Mobile computing 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
- Ensure portable and mobile computing 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 computing Team, fully licensed and only carried out by your computing Team
- In areas where there are likely to be members of the general public, portable or mobile computing 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
- As far as is reasonably practicable, keep with you at all times any computer or other equipment on which you do School's work when not in use. Where this is not practicable, such equipment should be safely secured and kept out of sight of others. Such equipment should never be left unattended in public places. It should not be left in sight in cars, public transport or public buildings such as hotels. They must not be left in vehicles overnight. When travelling you must always carry them in hand luggage.

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 during non contact time with students. At other times these must be switched to silent.

- Students are allowed to bring personal mobile devices/phones to school but these must be collected by the teacher and stored for the duration of the school day.

- The school is not responsible for the loss, damage or theft of any personal mobile device belonging to either staff or students.

- Staff should not use their own mobile phones to phone parents.

Mobile Phones

- When in your possession, you are responsible for the security of the 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
- School SIM cards must only be used in school provided mobile phones

- You must not send text messages to premium rate services
- If you have no other choice but to use the school mobile for personal means please advise the School Business Manager as soon as possible to arrange reimbursement.

Details of ALL On-Line Safety incidents to be recorded by the On-Line Safety coordinator. This incident log will be monitored by the Principal, Member of SLT or On-Line Safety Governor.

On-Line Safety incident log

South End Junior School, Wymington Road, Rushden, Northamptonshire

NN10 9JU Tel: 01933 314611

On-Line Safety Lead and contact details	
Details of incident	
Date and time	
Where did the incident occur?	
Name and contact details of person reporting the incident	
Who was involved in the incident (please specify)	☐ child/young person ☐ staff member ☐ other (please specify)
Names and contact details of those involved	
Type of incident (please select)	☐ Bullying or Harassment ☐ Online bullying or harassment (cyberbullying) ☐ Sexting (self-taken indecent imagery) ☐ Deliberately bypassing security or access ☐ Hacking or virus propagation ☐ Racist, sexist or homophobic religious hate material ☐ Terrorist material ☐ Other (please specify)

Description of incident		
Nature of incident	☐ Deliberate access ☐ Accidental access	
Did the incident involve material being….	☐ created ☐ viewed ☐ printed ☐ shown to other/s ☐ transmitted to others ☐ distributed	
Could this incident be considered as	☐ Harassment ☐ Grooming ☐ Cyberbullying ☐ Sexting (self-taken indecent imagery) ☐ Breach of AUP ☐ Other (please specify)	
Action Taken: (please specify)	**STAFF** ☐ Incident reported to Head/ Manager ☐ Advice sought from children's social care ☐ Incident reported to the police ☐ Incident reported to CEOP ☐ Incident reported to Internet Watch Foundation ☐ Incident reported to IT ☐ Disciplinary action to be taken ☐ On-Line Safety policy to be reviewed/amended	**CHILD/ YOUNG PERSON** ☐ Incident reported to member of staff ☐ Incident reported to social networking site ☐ Incident reported to IT ☐ Child's parents informed ☐ Disciplinary action taken ☐ Child/young person debriefed ☐ On-Line Safety policy to be reviewed

On-Line Safety incident log

What is the outcome of the incident/ investigation

What is the learning from the incident/ investigation

Recommendations and timescales to implement any amendments/actions

Signed		Print Name Date	
Signed		Print Name Date	
Signed		Print Name Date	
Signed		Print Name Date	
Signed		Print Name Date	
Signed		Print Name Date	

Appendix 2

INAPPROPRIATE USE

In the event of staff misuse

If an employee is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, a report must be made to the Head teacher/Safeguarding lead immediately. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:
Schools Senior HR Advisory Team
LADO (Local Authority Designated Officer)
Police/CEOP (if appropriate)

In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed only if appropriate.

Examples of inappropriate use

Accepting or requesting pupils as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers with students.

Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.

In the event of inappropriate use by a child or young person

In the event of accidental access to inappropriate materials, students are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action. Template student Acceptable Use Rules can be found in the appendix 3.

Students should recognise the CEOP Report Abuse button (www.thinkuknow.co.uk) as a place where they can make confidential reports about online abuse, sexual requests or other misuse which they feel cannot be shared with employees.

Appendix 3

SOUTH END JUNIOR SCHOOL

Acceptable Use Policy for Key Stage 2 Pupils

- I will ask permission before using the Internet and school equipment.
- I will look after all the school IT equipment and use it properly
- I will only access the system with my own password, which I will keep secret.
- I will not look at or delete other people's files.
- I will only put my own work on the internet
- I will not send messages which upset other people
- I will always ask before downloading from the internet or using material I have brought into school because I understand the risks from virus infections
- I understand that the school may talk to my parent or carer if they are worried about my On-Line Safety.
- I will use the computers only for schoolwork and homework.
- I will not bring USB sticks or software into school unless I have been given permission.
- I will only message people I know, or my teacher has approved.
- The messages I send will be polite and responsible.
- I will not lie about my age to get onto websites e.g. social media.
- I will not give my name, home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission.
- I will not use Internet chat-rooms.
- I will report any unpleasant material or messages sent to me. I understand my report will be confidential and will help to protect other pupils and myself.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I break these rules I may not be allowed to use computers or the Internet.

Child's name:

I accept the above statements and agree to follow these rules to ensure the safety of myself and others' at all times.

Signature:……..