South End Infant School	Acceptable Use Policy for Schools-based Employees and Pupils	South End Infant School SEIS ENGAGE EXPLORE ENQUIRE
This Policy is being reviewed by the Governing Body		Coordinator: **C Welford**
		Review Date: **Oct 2022**

1. Policy Statement

In order to create a safe teaching and learning environment, effective policies and procedures that are clearly understood and followed by the whole school community are essential. This Acceptable Use Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of **all technologies** to safeguard adults, children and young people within a school. The policy recognises the changing nature of emerging technologies and highlights the need for regular review to incorporate developments within ICT. This policy explains procedures for any unacceptable or misuse of these technologies by adults or children. E-Safety is a school community responsibility. It is the shared responsibility of all staff, parents and pupils. The view of parents and pupils help to shape how we keep pupils safe. Pupils will be taught to understand acceptable and unacceptable behaviour when using technology during planned and directed lessons, assemblies and circle times, and they will be taught how to report inappropriate use. The School Council and Cyber Crew will deliver training to pupils and parents, supported by the E-Safety Lead.

Why we have an Acceptable Use Policy (AUP)?

The use of the Internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children use these technologies. These risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- On-line content which is abusive or pornographic.

Whilst the school acknowledges that we will endeavour to safeguard against all risks we may never be able to eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure children continue to be protected. It is the duty of schools to ensure that children are protected from potential harm both within and beyond the school environment. Therefore, the involvement of children and parent or carers is vital to the successful use of online technologies. This policy aims to inform how parents/carers and children are part of the procedures and how children are educated to be safe and responsible users. The term 'E-Safety' is used to encompass the safe use of all on-line technologies in order to protect children and adults from potential and known risks.

The purpose of the Acceptable Use Policy is to identify for the whole school community:

- The steps taken in school to ensure the safety of pupils when using the internet, e-mail and related technologies.
- The school's expectations for the behaviour of the whole school community whilst using the internet, e-mail and related technologies within and beyond school.
- The school's expectations for the behaviour of staff when accessing and using data.

2. Scope of policy

The policy applies to all school based employees, including individuals working in a voluntary capacity. All schools are expected to ensure that non- employees on site are made aware of the expectation that technologies and the internet are used safely and appropriately. The Acceptable Use Policy should be used in conjunction with the school's disciplinary procedures and code of conduct applicable to employees and pupils.

Where this policy is applied to the Head Teacher, the Chair of Governors will be responsible for its implementation.

3. Legal background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of all school employees in relation to use of technologies feature within the following legislative documents, which should be referred to for further information:

The Children Act 2004

School Staffing (England) Regulations 2009

Working Together to Safeguard Children 2018

Education Act 2002

Safeguarding Vulnerable Groups Act 2009

GDPR in Schools/Data Protection "A Toolkit For Schools" April 2018

Also see Data Protection Policy

All safeguarding responsibilities of schools and individuals referred to within this Acceptable Use Policy includes, but is not restricted to the legislation listed above.

4. Responsibilities

Head Teacher and Governors

The Head teacher and Governors have overall responsibility for E-Safety as part of the wider remit of safeguarding and child protection.

To meet these responsibilities, the Head Teacher and Governors have:

- appointed a Designated E-Safety Lead to implement agreed policies, procedures, staff training, and curriculum requirements and take the Lead responsibility for ensuring E-Safety is addressed appropriately. All employees, pupils and volunteers should be aware of who holds this post within school.
- Provide resources and time for the E-Safety Lead to update protocols where appropriate and to be trained employees.
- Promote E-Safety across the curriculum and have an awareness of how this is being developed and if necessary added to the School Improvement Plan
- Share any E-Safety progress and curriculum updates at all governing body meetings and ensure that all present understand the link to child protection.
- Ensure that E-Safety is embedded within all child protection training, guidance and practices.
- Elect an E-Safety Governor to challenge the school about E-Safety issues and GDPR.
- Run E-Safety workshops and talks for parents.
- With the support of the IT Technician ensure the appropriate software and hardware, which facilitates safe storage and transportation of data, is provided to staff and children. Encryption/GDPR (Bit Locker and Encrypted USB pens).
- Provide server staff photocopier password protected mailboxes to allow safe sending and printing of personal data.
- To appoint a designated Data Protection Officer (DPO) LGSS
- To report serious data breech incidents to the LGSS DPO (see GDPR Schools Toolkit)
- Make employees aware of the Northamptonshire Safeguarding Children Partnership (NSCP) http://www.northamptonshirescb.org.uk/

E-Safety Lead

The nominated E-Safety Lead:

- Devises and delivers regular school E-Safety assemblies involving all pupils and staff.
- Recognises the importance of E-Safety and understands the school's duty of care for the safety of their pupils and employees.
- Runs E-Safety workshops and talks for parents.
- Ensures that up to date resources and materials regarding E-Safety are accessible to parents on the school website, along with links to CEOP and NSPCC.
- Establishes and maintains a safe IT learning environment within the school.
- Ensures that all individuals in a position of trust who access technology with pupils understand how the filtering levels operate.
- Ensures the computing curriculum integrates E-Safety; assemblies cover E-Safety and a progressive curriculum is taught regarding E-Safety and 'Netiquette' across the school.
- Checks pupils understanding through questioning and solicit pupils' ideas to maintain and improve E-Safety within year groups and the school.
- Train pupils to train the school on E-Safety, deliver CEOP teaching/training (Cyber Crew)

and support the School Council and Cyber Crew on monitoring E-Safety within the school.

- With the support of the Computer Technician or IT Subject Leader, ensure that filtering is set to the correct level for employees, young volunteers, children and young people accessing school equipment.
- Set up secure Teacher Learning Platform workspaces, with high privacy settings, to provide safe cloud data storage.
- Monitor the use of the Learning Platform/Purple Mash and class tablets.
- Report issues of concern and update the Head Teacher on a regular basis.
- Liaises with the Anti-Bullying, Child Protection and IT Leads so that procedures are updated and communicated, and take into account any emerging E-Safety issues and technological changes.
- With the support of the Computer Technician ensure transportable devices (laptops/tablets/zip drives/USB pens) are password protected and encrypted (Bit Locker).
- Co-ordinates and delivers employee training according to new and emerging technologies so that the correct E-Safety information is being delivered including GDPR.
- Maintains an E-Safety Incident Log to be shared at agreed intervals with the Head Teacher and Governors at governing body meetings.
- With the support of the Computer Technician or IT Lead, implement a system of monitoring employee and pupil use of school issued technologies and the internet where appropriate.
- Ensures that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensures that unsolicited e-mails to a member of staff from other sources is minimised (spam block controls) Refer to section 12 of the Allegation Procedure, NSCP, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Implement measures to ensure transportable devices and mobile devices have safety software/encryption and comply with GDPR 2018.

Individual Responsibilities

All school-based employees, including volunteers, must:

- Take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly. They must ensure that devices and software worked on outside the school are safe. They must keep up to date with training and be aware of the risks if using personal data. This includes transportation of data and working remotely. See DfE Data Protection "A Toolkit For Schools" April 2018 page 33.
- Ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner. Children should be informed about what to do in the event of an E-Safety incident.
- Ensure that they know who the Designated Safeguarding Lead is within school or other setting so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Head Teacher.
- Report any E-Safety incident, concern or misuse of technology to the E-Safety Lead or Head Teacher, including the unacceptable behaviour of other members of the school community.

- Ensure that children are protected and supported in their use of on-line technologies so that they know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- Be up-to-date with E-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Use school IT systems and resources for all school related business and communications, particularly those involving sensitive pupil data or images of Pupils. School issued email addresses, mobile phones and cameras must always be used by employees unless specific permission to use a personal device has been granted by the Head Teacher, for example, due to equipment shortages.
- Ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with their professional role and in line with school protocols. Personal details, such as mobile number, social network details and personal e-mail should not be shared or used to communicate with pupils and their families.
- Not post online 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. Individuals working with children and young people must understand that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites.
- Protect their passwords and personal logins, and log-off the network wherever possible when leaving workstations unattended in order to protect sensitive data and comply with GDPR (PCs automatically log off after 5 minutes).
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the Internet on a regular basis, especially when not connected to the school network.
- To change or update their profile password and ensure it remains secret.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies
- Understand that network activity and online communications on school equipment (both within and outside of the school environment) may be monitored, including any personal use of the school network. Specific details of any monitoring activity in place, including its extent and the manner in which it is carried out, should be detailed in the school's local IT Policy.
- Understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.

5. 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 or Designated Safeguarding Lead immediately. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

Schools Senior HR Advisory Team
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 pupils.
- Behaving in a manner online that 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, pupils are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action. Pupil Acceptable Use Rules and example sanctions can be found in the appendix.

Pupils should recognise the CEOP Report Inappropriate material button (www.thinkuknow.co.uk), Hector Protector and the Whistle (DB Primary) as a place where they alert adults. They should also know about the CEOP report Abuse button so they can make confidential reports about online abuse, sexual requests or other misuse that they feel cannot be shared with employees.

6. Policy Review

The Acceptable Use Policy will be updated yearly to reflect any technological developments and changes to the school's ICT Infrastructure. Acceptable Use Rules for pupils should be consulted upon by the School Council to ensure that all children can understand and adhere to expectations for online behaviour.

7. Use of specific technologies and support

Internet use

We teach our children and young people how to use the Internet safely and responsibly for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through ICT where the following concepts, skills and competencies have been taught by the time they leave

Year 2:

- Internet literacy
- making good judgements about websites
- knowledge of risks such as viruses and opening mail/messages/images from a stranger
- uploading information – know what is safe to upload and not upload personal information
- where to go for advice and how to report abuse

Most pupils recognise the need to be safe and act responsibly when using digital communications. Children are taught the SEIS internet rules, the school Cyber Crew review these regularly with the E-Safety Lead (these are displayed throughout the school and reminders are given during whole school assembly time and computing sessions).

The www.thinkuknow.co.uk resources are used, with free training provided to teachers/adults for the delivery of these lessons. Pupils recognise and refer to CEOP Lee, Kim and SID, Jessie and Friends, online safety rules. They also access Online Safety through Purple Mash units.
These skills and competencies are taught within the curriculum so that children have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner.
Children will know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information including:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address
- school
- clubs attended and where
- age or DOB
- names of parents
- routes to and from school
- identifying information,

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded. Pupils should also be taught what type of images are acceptable/unacceptable to be uploaded/shared. Pupils need to know how to protect themselves.

Learning Platform – Also see Purple Mash Literature
Purple Mash provides a wealth of opportunity for adults and children within and beyond school to:

- collaborate and share work via web cams and uploading
- ask questions
- debate issues
- dialogue with peers
- dialogue with family members or carers
- access resources in real time
- access other people and cultures in real time
- develop an on-line community

The tools available for use within the learning platform for adults, children include:

- Internet access
- E-mail
- Video-conferencing
- Weblogs (on-line diaries)

- Wikis (on-line encyclopaedia or dictionary)
- Instant Messaging
- An on-line personal space for adapting as a user to:
    - upload work
    - access calendars and diaries
    - blog

The personal space contains some information about the user. Parents and Staff should teach pupils to use their login and password, keeping them secret, to access the LP/Purple Mash. (Such as a social networking site SNS/messenger apps e.g. Instagram, Snapchat, Whatsapp, Twitter and Facebook) and should reflect key messages for any on-line use. When using the LP staff and parents should discuss pupils always consider the risks and consequences of anything they may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

E-mail use

Staff, children and young people are to use their school issued e-mail addresses for any communication between home and school only.

Parents/carers are encouraged to be involved with the monitoring of E-mails sent, although the best approach with children is to communicate about who they may be talking to and assess risks together.

Teachers are expected to monitor their class use of E-mails Gmail and Purple Mash/Tapestry where there are communications between home and school, on a regular basis.

Video-conferencing

The use of web cams to video-conference will be via the learning platform which is a filtered service. Trained staff will supervise this at all time. Where children and adults may be using a web cam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Rules.

Taking images via a web cam will follow the same procedures as taking images with a digital or video camera.

Mobile Phone – also see separate Mobile Phone Policy for Staff/Volunteers.

Staff members are not allowed to use their personal numbers to contact children under any circumstances.

It is also our policy to ensure that we educate our children in understanding the use of a public domain and the consequences of misusing it including the legal implications and law enforcement through relevant curriculum links.

Other technologies schools use with children and young people are:

- *Photocopiers*
- *fax machines*
- *telephone*

Video and photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

The personal space on the learning platform should not have personal photographs uploaded

that reveal more than a general location, an activity (without close-ups of children's faces) or piece of work, without the express permission of parents/carers and school.
It is also highly recommended that permission is sought prior to any uploading of images to check for inappropriate content.
The sharing of photographs via weblogs, forums or any other means on-line will only occur after permission has been given by a parent/carer or member of staff.
Photographs/images used to identify children in a forum or using Instant Messaging within DB will be representative of the child rather than of the child e.g. an avatar.
Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name although Child Protection Guidance states either a child's name or a photograph but not both. Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit. Photographs will be stored carefully and are only accessible to key staff with passwords.

Filtering and safeguarding measures
Staff and children are required to use the personalised learning space and all tools within it, in an acceptable way.
Please refer to the Acceptable Use Rules for Staff and children and young people for the appropriate use of the learning platform.
The broadband connectivity has a filter system which should be set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. **All** filtering is set to 'No Access' within any setting and then controlled via: Portal Control (controls filtering at local site level) which controls individual access to the Internet.

Support
The school will send home guidelines on the use of the internet, emails and online technology at home and at school. The school website E-Safety page is regularly signposted to parents/carers and contains appropriate information and professional links/guidance. E.g. Thinkyouknow, NSPCC and Childnet.
They will be told about Childnet International 'KnowITAll for Parents' on-line materials (http://www.childnet.com/resources/kia/) to deliver key messages and raise awareness for parents/carers and the community. This will help them find out how to use the tools their children are using.
The Appendices detail where parents/carers can go for further support beyond the school. The school will endeavour to provide access to the Internet for parents/carers so that appropriate advice and information can be accessed where there may be no Internet at home, subject to arrangement.

South End Infant School

Acceptable Use Rules for staff.

2021-2022

These rules apply to all on-line use and to anything that may be downloaded or printed. To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves. It will also ensure we educate pupils on the safe and acceptable use of technology.

- I have read and understand the SEIS acceptable use/e-policy document; I understand there are procedures/sanctions in place to ensure safe online practices.
- I know the school internet E-Safety rules and/or where to find them.
- I will encourage and educate pupils on how to and who to report cyberbullying or inappropriate images/content.
- I will encourage children to report worries/concerns involving online stranger danger to a trusted adult.
- I will read risk assessments and follow guidance.
- I know that E-Safety is the responsibility of all within the school community, staff, parents and pupils and I have been informed about GDPR. I will report any breech of data protection to the Esafety Lead, Headteacher and Cluster Data Protection Officer.
- I will model what is acceptable and unacceptable when using technology and the www.
- I will use my School GMail email for school and professional email.
- I will attend whole school E-Safety assemblies to keep up to date with E-Safety education and resources. I am familiar with the CEOP E-Safety curriculum. I have the knowledge required to ensure E-safety is explored appropriately in school.
- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I will update my profile password and keep it secret and I will always log off when leaving any device unattended.
- I will not share my work profile with any other member of staff (GDPR).
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Internet or send them via E-mail and I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.

- I will report accidental misuse and I will report any incidents of concern for children's or young people's safety to the Head Teacher, Designated safeguarding Lead or E-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I will record/report incidents of cyber bullying; reporting to the Head Teacher, Designated Safeguarding Lead or E-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Safeguarding Lead is.
- I know who the E-Safety Lead is and how to report cyberbullying, abuse of the Purple Mash/Tapestry Learning Platform and who to speak to if a child is/or has been put at risk using www/LP.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Head Teacher and/or E-Safety Leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I know the Google Classroom/Google Drive platform is the safest place to store information about school and I will protect my password.
- If sensitive information is stored on a transportable device it will be encrypted or password protected.
- I will ensure that I follow the Data Protection Act 2003 and have checked I know what this involves.
- I will only install hardware and software for which I have been given permission.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the E-Safety Leader.
- I have been given a copy of the Acceptable Use Policy to refer to about all E-Safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.
- I have received regular E-Safety training and information to highlight the risks to my own and pupil online safety. I know who to go to if I have any further questions.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of E-Safety and my responsibilities to safeguard children and young people when using on-line technologies. It is the responsibility of all staff to keep up to date with E-Safety developments and monitor pupil safety.

Signed……..Date…….

Name (printed)……

School…….*South End Infant School, Rushden*…….....

South End Infant School
SEIS
ENGAGE EXPLORE ENQUIRE

Email: seis.southend.northants@dbprimary.com

Head teacher:
Mrs E Ashcroft

Telephone No. 01933 356571

Wymington Road
RUSHDEN
Northamptonshire
NN10 9JU

Deputy Head teacher:
Mrs S Ireton

E-Safety Acceptable Use Rules Letter to Parents/Carer for Primary

Dear Parent or Carer,

As part of an enriched curriculum your child will be accessing the Internet, E-mail and personal on-line space via Purple Mash/Tapestry. In order to support the school in educating your child about E-Safety (safe use of the Internet), please read the following Rules with your child then sign and return the slip. In the event of a breach of the Rules by any child, the E-Safety Policy lists further actions and consequences, should you wish to view it. These Rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home). Should you wish to discuss the matter further please contact the school.

For more online information visit our school E-Safety website and CEOP or NSPCC or www.**thinkuknow**.co.uk *(CEOP Child Exploitation and Online Protection Agency)*

Yours faithfully,
Mrs E Ashcroft

……

Parents/carers – also see documents in the letter section of the school website.

E-Safety Pupil Agreement (Acceptable Use)

South End Infant School Cyber Rules.

(Written by the pupils, agreed by our "Cyber Crew" and School Council).

We use the internet when we are with an adult. We know we have to be careful. We only go on sites our adults have checked first.

We keep our **personal information** a secret when online:
- we don't tell people our full name.
- we don't tell anyone our address or the school we go to.
- we don't send photos on the internet/online.
- we keep our passwords safe.

We are **Stranger Aware**. When we are online, we only talk to people we know in real life.

If we find a website/image/video, we don't like, we **tell a trusted adult** straight away.

We are **ALWAYS polite and friendly** in the real world and online.

If someone upsets one of us online, we know who to ask for help. We know to **report our worries** instead of trying to fix it on our own.




Pupil Name: _____

I agree to follow our school internet rules, to stay safe online.

Signed:_____

Date:_____