South End Junior School	**Page 1 of 17**
	Issued: 13 October 2020 **Updated: 7 December 2020**
On-Line Safety & Acceptable Use Policy	**Review date: Autumn 2021**
	Supersedes: 20 November 2019
Approved by	~~FULL GOVERNING BODY~~/L & M COMMITTEE/~~HEADTEACHER~~

Introduction

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

This policy has been written in compliance with the 'Guidance for safer working practices for adults working with children and young people in educational settings 2019'.

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, Instagram 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 will sign an acceptable usage policy (Appendix 3), which parents will have sight of.

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. The school has a Data Security Policy which must be read in conjunction with this policy. Staff will sign an acceptable usage policy when they join the school (Appendix 4).

Both this policy is 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 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.

How on-line safety is covered in the Curriculum

The school links its online safety teaching closely to PSHE, Open minds and Computing Long Term Overview. The school also uses Be Internet Legends to provide accompanying Online Safety lessons to the Computing lessons. Online safety is reinforced as often as possible and not only during online safety talks, and days.

The Be Internet Legends programme gives teachers the tools and methods they need to teach online safety fundamentals in the classroom. Inside this booklet you'll find a full set of lesson plans. Two have been written for the younger children in your school (years 3 and 4: ages 7-9), while the rest were created for older children (years 5 and 6: ages 9 -11). These plans provide fun, age-appropriate learning experiences around four internet safety pillars: • Think Before You Share (Be Internet Sharp) • Check it's For Real (Be Internet Alert) • Protect Your Stuff (Be Internet Secure) • Respect Each Other (Be Internet Kind) The fifth pillar brings everything together. It provides interesting and valuable follow-up discussions to have in class or during a regular safeguarding discussion. • When in Doubt, Discuss (Be Internet Brave)

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
- Raw image searching is strictly filtered on results.
- 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).

The school uses a product called SurfProtect Quantum to provide its internet content filtering service, which is Prevent Duty compliant. This also enables the school to identify inappropriate searches that the system has blocked.

The filtering service offers:-

- Different filter profiles for different users/user groups or individual machines.
- Categorisation of websites based on content displayed, with certain categories being automatically blocked, whilst allowing certain sites to be blocked or unblocked.
- HTTPS filtering giving a more in-depth level of protection, eg. results when users search on YouTube can be filtered, allowing the user to completely cut out inappropriate video content, whilst still allowing access to educational videos on the site.
- Any given social media sites can be easily blocked.

E-Mail

Children will have access to individual office 365 email accounts. This is in light of Covid-19, and the need to provide remote learning for all pupils.

These email accounts have been generated through the DfE funded program and company "Turn it On" recommended by Easi-PC.

Restrictions have been put in place, such as:

- Emails from/to external sources will be blocked
- All emails sent from a child's account will be sent with a DSL copied in
- APPS on Microsoft and TEAMS will be limited to key adults only
- All children will have an individual email address and password
- Only key members of staff will have password manager access
- An Email Catcher system will be put in place

Remote Learning

In light of Covid-19, remote learning will take place through Microsoft TEAMS.

Children have been given safeguarding instructions on how to manage emails and use TEAMS safely and appropriately.

Staff need to:

- Ensure that a member of SLT knows which/that the/an online lesson is taking place, and for what purpose
- Blur out the background in video sessions and dress following the Code of Conduct

- Avoid one on one situations with pupils whilst on TEAMS – staff need to request that a member of SLT join the session, or that a parent is present in the room
- Only record a lesson or online meeting with a pupil where this has been agreed with the headteacher or other member of SLT, and the pupil and their parent/carer have given explicit written consent to do so
- Be able to justify images of pupils in their possession

STAFF USING TEAMS 365

- Adults do not allow children to present work
- The children must wait in the lobby until the teacher invites them in
- Teacher to download a list to see who was present in every session
- Any safeguarding issues to be reported immediately to a DSL
- Only pupils should be seen by the class teacher, not adults.

Adults should not:

- Contact pupils outside the operating times defined by senior leaders
- Take or record images of pupils for their personal use
- Record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by senior staff)
- Engage online while children are in a state of undress or semi-undress

Roles and Responsibilities

This policy, supported by the school's Data Protection and Data Security 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 Gurdip Kaur and the On-Line Safety Governor is Margaret Barnes. All members of the school community will be made aware of who holds these posts.

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.

- 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 Head on a regular basis.

- Liaise with the Anti-Bullying, Child Protection and computing leads so that procedures are updated and communicated, and consider 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 where appropriate.

- 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.

Staff and Volunteers

- Protect the security and confidentiality of school networks and systems**.**

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, 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 for downloads and email attachments. For instructions on how to carry out a virus scan on a removable media please see the Data Security Policy.

- 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 report it in the usual way.

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.

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, and Management Information System log-in username. Further information is available in the school's Data Protection and Data Security Policies.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and systems**.** 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 are signposted to sites that will give them guidance on using social networking safely, as follows:-

https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/teaching-resources/social-media-checklists

https://swgflstore.com/

Staff using social networking sites:-

- Are encouraged to ensure that their privacy settings are set to maximum
- Should be aware that behavior in their personal life may impact upon your work with children
- Should think about changing their Facebook profile picture and username to keep prying eyes out. E.g. Use a cartoon image and a nickname.
- Should seek advice from the Headteacher if they are contacted by pupils or ex-pupils under the age of 18, unless the family is a genuine friend or family member of staff.
- Should follow the school's Social Media Policy when posting on or setting up any school social media sites.
- Should follow the school's Code of Conduct.

Staff using personal social networking sites should not:-

- Use or access social networking sites of pupils unless they are close family or friends.
- Use or access social networking sites of ex-pupils under the age of 18 years unless they are a family member.
- Give their personal contact details to pupils, including their mobile telephone number/email (unless the family is a genuine friend or family member of staff)
- 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 Head 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.
- Post photographs/pictures of pupils on their social networking site unless close family.
- Post photographs/pictures of staff - unless the staff member has given them permission – on the social networking sites

Safe Use of Images

Taking of Images

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. The Data Protection Act 2018 requires the school to have a lawful basis for processing data. If an image is being used for any of the following reasons, South End Junior School requires consent to use these mages for communication, marketing and promotional materials.

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 communication, marketing and promotional materials. This may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Inclusion in the school's prospectus.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

On entry to the school, all parents/carers and staff will be asked if they give permission for images to be used as above. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. If consent is withdrawn after a photograph has been used in a publication or on-line, we will continue to make use of the publication(s) incorporating the photograph and/or on-line facility but we will not use the photograph again and will remove it from the publication if it is re-printed.

Before using an image of a person for the following purposes, a check needs to be made to ensure that permission has been given for: -

- Website
- Prospectus
- Internal display
- Social media
- Blogs
- External newspaper
- School Newsletters of any kind

Use of an image on other mediums where consent would be required will need to obtained at the time of use.

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.
- Any image of pupils that is on a staff member's personal device and personal cloud-based storage or server must be deleted within 48 hours of the event/return from trip.
- Images of pupils should be deleted from staff iPads or H Drives on computers. If they need to be retained they should be moved to the T Drive.
- Images should be deleted in accordance with the school's Data Retention Schedule.

School computing Equipment

- As a user of computing, you are responsible for any activity undertaken on the school's computing equipment provided to you.
- All activities carried out on School systems and hardware will be monitored in accordance with the general policy.
- 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 date should not be stored on the local drives of desktop PCs (C drive). If it is necessary to do so, the local drive must be encrypted wherever possible.

- 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).
- Staff must follow the school's Data Security Policy.

Portable & Mobile computing Equipment

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 laptops, iPads 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.

<u>Staff computing equipment</u>

- 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.
- 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.

- Staff use of Microsoft TEAMS will mean resources are shared with children, but personal data will not be. Staff Teams have different security settings to ensure data is kept safe.

Pupil computing Equipment

Pupils are required to log on to school computing Equipment that they may use. This will enable the school's third-party monitoring software to identify the user when monitoring occurs.

Mobile Technologies

Mobile phones – Bring Your Own Device

- 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 and out of sight.
- 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.
- COVID -19 has meant that staff do not collect in any mobiles phone to reduce the risk of unnecessary transmission.
- 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.
- COVID-19 has meant that parents are not meeting teachers face to face. Teachers can use their own mobile phones to call parents HOWEVER caller ID is off and this is checked by the DOL before the call is made.
- The school allows staff to use their own personal mobile devices to take images of pupils on behalf of the school whilst on a trip, residential trip or at a school even AND the school's mobile phone is not accessible AND images are then deleted in accordance with instructions on "Storage of Images".
- The school allows staff to access their emails on their own personal mobile devices. However, the school's Data Security Policy must be followed.

Mobile phone – school phone

- When in your possession, you are responsible for the security of the school mobile phone. The PIN code should not be deactivated on the school mobile phone and it should not be left 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 use my email account responsibly: keeping my password a secret, and only sending messages to approved people.
- I will report any suspicious emails I receive to a trusted adult
- 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.
- I will ask an adult for help if I am not sure whether I am using trusted sites.
- My behaviour online should be as good as my behaviour offline.
- When using TEAMS 365
    - I must pin the teacher so he/she can be seen
    - I have the video off, and sound muted when entering a meeting
    - I am not allowed to present work
    - I only post comments in line with our school values

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:……..

Appendix 4

SOUTH END JUNIOR SCHOOL

Acceptable Use Policy for Staff at South End Junior School

- I am aware that the school has a Data Security Policy and I will follow this policy.
- I am aware that the school has a Social Media Policy and I will follow this policy.
- I am aware that the school has an Online Safety Policy and I will follow this policy.
- I am aware that the school has a Code of Conduct and that this Code outlines expectations for photography, videos & other images, as well as use of technology, which I will follow.
- I am aware that I am permitted to access work emails on my personal mobile phone but that I should follow security measures outlined in the school's Data Security Policy.
- I understand the expectations upon me if I use my personal device to take images of children and am aware of the circumstances in which I am permitted to do this.
- I 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.
- I will ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with my professional role and in line with school protocols.
- I understand that what I post online or via social networking sites could compromise my position within the work setting.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

Staff'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:…….. Date ……