E-Safety & Acceptable Use Policy

Governors' Committee Responsible:	**Children & Learning Committee**
Nominated Lead Members of Staff:	**Headteacher / ICT Leader / CEOP Leader**
Status & Review Cycle:	**Recommended (Every 2 years)**
Next Review Date:	**Autumn 2025**

Introduction:

E-safety is defined as being safe from risks to personal safety and wellbeing when using all fixed and mobile devices that allow access to the internet, as well as those that are used to communicate electronically. This includes personal computers, laptops, mobile phones, digital cameras, wearable technology (such as smartwatches) and gaming consoles such as Xbox, Playstation and Nintendo Switch.

Safeguarding against these risks is not just an ICT responsibility, it is everyone's responsibility and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable.

Our E-safety Policy has been written by the school, involving all stakeholders and builds on best practice and government guidance. It relates to the latest version of DfE statutory guidance: **'Keeping Children Safe in Education'**, and **Surrey Safeguarding Children Partnership 5.35 Online Safety Guidance**.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our **Anti-bullying Policy** and **Behaviour Policy**.

Understanding the risks of using the Internet and associated devices:

The internet is an essential element in 21st century life and ICT knowledge, now seen as an important life-skill, is vital to access life-long learning and employment. It is also important to recognise that the internet provides many benefits, not just to children, young people and vulnerable adults, but also to the professional work of staff.

E-Safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of E-Safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-Safety is a whole-school issue and responsibility.

While acknowledging the benefits, it is also important to recognise that risk to safety and well-being of users is ever-changing as technologies develop. These can be summarised as follows:

Content

- Commercial (adverts, spam, sponsorship, personal information)
- Aggressive (violent/hateful content)
- Sexual (pornographic or unwelcome sexual content)
- Values (bias, racism, misleading info or advice)

Contact

- Commercial (tracking, harvesting personal information)
- Aggressive (being bullied, harassed or stalked)
- Sexual (meeting strangers, being groomed)
- Values (self-harm, unwelcome persuasions)

Conduct

- Commercial (illegal downloading, hacking, gambling, financial scams, terrorism)
- Aggressive (bullying or harassing another)
- Sexual (creating and uploading inappropriate material, including sexting)
- Values (providing misleading info or advice)

Much of the material on the internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime, racism and extremism that would be considered inappropriate and restricted elsewhere.

It is also known that adults who wish to abuse others may pose as a child/young person/peer to engage with them and then attempt to meet up with them. This process is known as 'grooming' and may take place over a period of months using chat rooms, social networking sites, tablets and mobile phones.

Cyberbullying:

Cyberbullying is bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages, emails or through messaging within social media websites. This bullying can be either personally or anonymously directed at individuals, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or email.

Sexting:

This involves users sending sexually explicit texts in the form of images or video to other children or adults. These images are often then distributed further without permission, which poses a significant safeguarding risk and places them at risk of further harm.

Why internet and digital communications are important:

Teaching and learning:

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- We believe that the use of Internet and is a necessary tool for staff and pupils. The children learn how to use the internet to find, search, exchange and share information.

- The school Internet access is provided by Surrey County Council and includes filtering set an appropriate level for pupils at our school. The level of filtering restricts access to inappropriate content but is not so restrictive that children and adults cannot access important tools for teaching and learning in school.
- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use. (As displayed through our '**think then click or tap poster'** – Appendix 1)
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content:

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

In addition to accessing the internet in organisation settings, children, young people and vulnerable adults may access the internet and/or use other digital technologies in their own time at other locations. This is when they will be at greater risk if they have not been taught about how to use them safely and what the dangers are.

Managing Internet Access & Roles and Responsibilities:

The school E-Safety coordinator is: Mrs Julie Hall (SLT and CEOP Trained)

The designated member of the Governing Body responsible for E-Safety & Safeguarding is: Mr Jack Robson

Governors

Governors are responsible for the approval of the E-Safety policy and for reviewing the effectiveness of the policy by reviewing e-safety incidents and monitoring reports. E-Safety falls within the remit of the governor responsible for Safeguarding. The role of the E-Safety Governor will include:

- Ensure an E-safety policy is in place, reviewed every 2 years (or earlier if required) and is available to all stakeholders
- Ensure that there is an E-Safety coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive
- Ensure that procedures for the safe use of ICT and the Internet are in place and adhered to
- Hold the Headteacher and staff accountable for E-Safety.

Headteacher and SLT

The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day-to-day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator. Any complaint about staff misuse must be referred to the E-Safety Coordinator at the school or, in the case of a serious complaint or allegation which breaches safeguarding procedures, to the Headteacher.

- Ensure access to induction and training in E-Safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.

- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SLT.
- Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured.
- Work in partnership with the DfE, Local Authority and the Internet Service Provider, Computing Leader and school IT Technician to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- The Senior Leadership Team will receive monitoring reports from the E-Safety co-ordinator.

E-Safety coordinator:

The E-Safety Coordinator will undertake relevant training, including the CEOP training to ensure the school is aware of the key messages in relation to keeping children safe online and ways to tackle child exploitation. This will also be complemented by regular training in line with the PREVENT duty to protect children from the risks of radicalisation and extremism. Other duties include:

- Leading E-safety staff meetings and workshops for parents.
- Works in partnership with the DfE, Local Authority and the Internet Service Provider, Computing Leader and school IT Technician to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of E-safety incidents and creates a log of incidents to inform future E-Safety developments.
- Liaise with the nominated member of the governing body & Headteacher to provide an annual report on E-Safety.

IT Technician:

The It Technician is responsible for ensuring:

- That the schools technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required E-Safety technical requirements and any relevant body E-Safety policy / guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant.
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher; E-Safety coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies.
- Updating of the relevant virus protection.
- Discussing security strategies with the Local Authority, Internet Service Provider and other link Governor.

Email:

- Pupils and staff may only use approved email accounts which will be checked to ensure they offer added protection of information sharing.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone they meet online.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.
- Staff to staff emails concerning children should use initials as identification, not full names.

Google Classroom:

- Class codes to access the classroom will only be shared between the teacher and pupils within school
- On the occasion a child leaves the school, they will be removed from the google classroom
- Comments will be monitored by the class teacher
- Pupils must not reveal personal details in communication
- Staff to pupil online communication must only take place via google classroom and will be monitored

Publishing pupil's images and work

Images or videos of children are considered to be forms of personal information:

Pupils' full names will be avoided on the school website, particularly in association with photographs. If a photo is used in any context, the child's full name should not be.

Written permission from parents or carers will be obtained before photographs or videos of pupils are used in school or published on the school website / in press. This will be obtained when the child joins the school to cover all uses, although a parent may withdraw their permission in writing at any time.

SD cards, memory sticks and CDs are a temporary means of storage for images. Once they have been used or uploaded to a secure location (e.g. the school network) they should be removed from the temporary storage device. Only encrypted memory sticks should be used for GDPR purposes.

Images obtained via a third party are subject to copyright and either verbal or written permission should be obtained before they are used.

During performances in school, parents and guardians will be reminded that photographs and videos taken must be retained only for their own personal use and not posted online without the express permission of all of the parents or guardians of the children shown.

Social networking and personal details:

The school uses social media to communicate with parents and the wider community. The school has its own twitter X feed: **@ShottermillJrs** which is used to share positive achievements by its pupils, staff or parents. It is also used (where appropriate) as a means of communicating updates to parents such as when children are out on an educational visit or residential trip. Updates from the school twitter feed also occur on the school's home page of its official website. The school does not respond to direct messages via twitter and parents will be directed to use the school telephone number or email address to get in touch.

In addition to this, the Parent Teacher and Friends Association have their own **PTFA Facebook Page** to directly communicate with parents. Strict codes of conduct are in place to ensure that this social networking site is monitored and managed properly. Inflammatory, negative comments about the school will be immediately dealt with by the Senior Leadership Team and in serious cases we may seek to involve the Police.

- As most social media applications and websites are for ages 13 years and upwards, the school will limit pupil access to these sites, and consider how to educate pupils in their safe use e.g. use of passwords.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering and access to inappropriate content:

- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved in line with the most recent guidance.
- If staff or pupils come across unsuitable online materials, the site must be reported to a member of the Senior Leadership Team.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Class Teachers will be responsible for overseeing the content that children access, particularly in places outside of the classroom (corridor computers or use of portable technologies) or at times outside of lessons (break times or after school clubs).

Managing emerging technologies:

- Emerging technologies will be examined for educational benefit and the potential risks assessed before use in school is allowed.
- Children will not be permitted to bring to school a personal mobile phone (or wearable technologies such as a Smartwatch).
- Games machines including the Sony Playstation, Microsoft Xbox and others which have Internet access which may not include filtering will be strictly monitored. Care will be taken with their use within the school.

Protecting personal data:

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The IT Technician will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- Files held on the school network will be regularly checked for viruses
- The use of user logins and passwords to access the school network will be enforced
- Portable media containing school data or programmes will not be taken off-site without specific permission from the Headteacher or Deputy Headteacher. All memory sticks used must be encrypted.

For more information on data protection in school please refer to our **data protection policy**.

Data Storage and Transport:

All personal information must be kept secure. At Shottermill Junior School we employ a combination of technical and procedural solutions to maximise the security of personal data (including photographs) of children or adults:

- All staff laptops will be password protected and staff will be encouraged to change these regularly.
- Transporting personal information off site should be avoided unless necessary.
- If personal data is required to be taken off site, it should either be stored on a password protected laptop or an encrypted memory stick and be deleted when no longer needed.
- An adult should take all necessary precautions when using a school laptop at home to make sure that no material is accessed which could contravene any elements of this policy (e.g. this has implications for uploading personal photographs, personal use of the internet, allowing other people to use the machine, etc.)
- Much of the school's planning and administrative tasks, including pupil data is stored securely within the Google Classroom drive, which is password protected. Teachers must ensure that passwords are not disclosed to any other person to themselves. The access to Google Classroom will be removed once an employee leaves the school.

Policy Decisions

Authorising Internet access:

1. All staff must read and sign the '**Staff Acceptable Use Agreement**' (See Appendix 2) before using any school ICT resource or personal device in school.
2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
3. Any child who is deemed a high risk when using the Internet or any ICT equipment / resource will have restricted access in school and in this exceptional circumstance, parents will be consulted on the management of ICT curriculum provision offered to their child.
4. Parents will be asked to sign and return a consent form.
5. Any person not directly employed by the school will be reminded of the school's 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site. Use of ICT resources will be monitored closely.

Assessing risks:

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will monitor ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints:

- Complaints of Internet misuse will be dealt with by a member of the SLT and recorded promptly on CPOMS.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the E-safety policy to pupils:

- Appropriate elements of the E-safety policy will be shared with pupils.
- E-safety posters will be posted nearby to where computers or mobile devices may be used.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils.

Staff and the E-safety policy:

- All staff will be directed to read the school's E-safety Policy and its importance explained.
- All members of staff will be asked to sign the **Acceptable Use Agreement**.
- Staff should be aware that Internet traffic is closely monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by SLT and have clear procedures for reporting issues.

Enlisting parents' support:

- Parents' and guardians' attention will be drawn to the School E-safety Policy in newsletters and will be made available on the school website.
- Parents' will be directed to useful information on the school website, including CEOP, PEGI rating system, Netaware and Parentinfo from NSPCC.
- Parents and carers will from time to time be provided with additional information on E-safety – such as parent workshops.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- In instances where the school has concerns about a child's home access to computers or online technologies including incidences of: Cyber-Bullying, meeting strangers, accessing inappropriate content such as video games above the recommended age certificate, the Child Protection Policy will be referred to and concerns dealt with in accordance with its procedures.

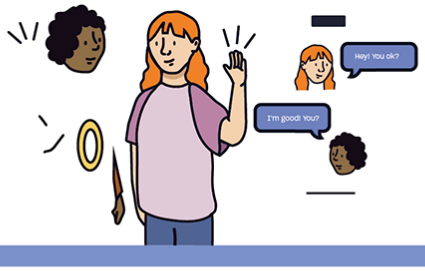
Appendix 1

High Speed Training™

TOP TEN TIPS TO STAY SAFE ONLINE

1 Don't share your personal information

2 Only talk to people that you know



3 Don't meet up with anyone you have only met online

4 Only accept friend requests from people you know personally

5 Always think carefully about what you post

6 Make use of the privacy settings on all of your social media accounts

7 Remember that not everyone online is who they say they are

8 Report inappropriate content immediately

9 Only share images that you'd be comfortable with your friends and family seeing

10 Never share your passwords

Appendix 2:

Shottermill Junior School

Acceptable Use Agreement

Governors' Committee Responsible:	**Children & Learning Committee**
Nominated Lead Member of Staff:	**Headteacher / ICT Leader / CEOP Leader**
Status & Review Cycle:	**Recommended (Every 2 years)**
Next Review Date:	**Autumn 2025**

Introduction

This Policy has been written by the school, involving all stakeholders and builds on best practice and government guidance. It relates to the latest version of DfE statutory guidance: **'Keeping Children Safe in Education'**, and **Surrey Safeguarding Children Partnership 5.35 Online Safety Guidance**.

This agreement should also be read in conjunction with the most recent version of the **Shottermill Junior School Staff Handbook,** which sets out the **Staff Code of Conduct**, use of electronic devices and social networking sites, safeguarding children and our expectations for upholding the highest standards of professional conduct both in and outside of the school workplace.

The aims of this policy are:

- To encourage safe use of the Internet by both children and adults working within our school.
- To encourage the development of skills to access, analyse and evaluate resources from the Internet.
- To use these resources to support teaching and learning across the curriculum.
- To ensure their supervised and appropriate use.

Guidelines:

As access can lead to any publicly available resources on the Internet, a filtered/screened service will be used in school to block access to the majority of unsuitable sites. This will ensure access to unsuitable material is minimised.

Children will be shown how to find and access information on suitable web search engines, such as 'Google'.

All staff members will be aware of their responsibilities towards pupils, checking sites they recommend are suitable, ensuring that access is supervised and that appropriate rules are being followed.

Whenever possible, screens should always be facing the teacher. Where this is not the case the teacher must walk regularly around the group to supervise sites being accessed. Children should be aware of the problems associated with Internet access and should be encouraged as a class to develop their own Internet rules before the class uses the Internet. They should know that by using 'history' and 'cookies', the teacher can review what has been accessed.

If possible, a written record is to be kept of any undesirable material that is accessed inadvertently. Contact with the ISP will be made if necessary to adjust filtering settings.

Emails:

Staff may be required to use the Microsoft Authenticator App to log into their email in school, as this provides the highest level of security protection. This means that staff may be required to access their phones in classrooms. Mobile phones should only be brought out for the time that is necessary to log into emails and should be locked away thereafter.

Staff email addresses are only available for staff to use. No email should be sent from the school without a member of staff approving it and to protect the wellbeing of staff, email communications are sent through the Office email address. Staff are requested to avoid sending emails to other staff outside of school hours, wherever possible, to protect work/life balance.

Google Classroom:

Google classroom is a key tool in online education. All communication with parents and students must relate to the work. Only private comments should be used, apart from specific circumstances (ie. art week, commenting on art work). This will be monitored by teachers and any inappropriate comments must be deleted.

Virus Protection:

Virus protection is installed and kept up to date in school (Sophos Anti-Virus). Computer users, especially Internet users, should be aware of the dangers of virus corruption from Internet downloads or attachments to emails. Daily virus updates to the school network will be used to help prevent damage to files and systems.

Internet and System Monitoring:

All Internet activity is monitored by the school system and checked by the school ICT technical support manager, as well as the Headteacher, Deputy Headteacher and E-Safety coordinator. It is the responsibility of those designated staff to review and respond to any breaches of the school's Internet policy and/or use of obscene, racist or threatening language detected by the system.

Any serious transgressions of the school's E-Safety Policy will be recorded and dealt in accordance with the school pupil Behaviour Policy, or for adults the Whistleblowing Policy and Staff Code of Conduct. Concerns should be reported immediately to the Headteacher (or in the case of the Headteacher, the Chair of Govenors) who will investigate and may follow up with the Local Authority Designated Officer (LADO).

Internet Publishing Statement:

The school wishes our website to reflect the range of activities and educational opportunities on offer at Shottermill Junior School, however, we recognise the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication, the following conditions should be adhered to:

- No photograph or video recording may be published without the written consent of the parents/legal guardian of the child concerned, and the child's own verbal consent.
- Surnames of children should not be published, especially in conjunction with photographic or video material;
- No link should be made between an individual and any home address (including simply street names);
- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in any doubt at all, refer to the person responsible for child protection.

Staff and Volunteers must abide by the following code of conduct:

ICT is seen as beneficial to all members of the School in supporting learning, teaching, research, administration and approved business activities of the School. The School's ICT facilities provide a number of integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users at the School. This could also lead to breaches of the data protection rights of a number of individuals causing harm to those individuals, and to the School.

This Acceptable Use Agreement is intended to ensure:

- that all users, will be responsible and stay safe while using ICT devices, systems and services.
- that school devices, systems, services and users are protected from accidental or deliberate misuse that could put the security of these systems and users at risk.

Key features of the e-safety policy will be outlined in the **Safeguarding Leaflet for Visitors.**

Agreement

- I understand that I must use School systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users, including as to the personal data of others.
- When using the School's ICT facilities:
- I understand that the School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have prior permission;
- I understand that the School may monitor my use of the devices, systems, services and communications at any time;
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it;
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details);
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line;
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);
- I will respect others' work and property and will not access, copy, remove or otherwise use or alter any other user's files, without the owner's knowledge and permission, and I will ensure that any use is in accordance with School policies;
- I understand there are risks when using the systems and services, and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials;
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will respect copyright of materials and intellectual property rights and not take or distribute text, images or other materials without permission;
- I will not use or modify any of the School devices, systems and services in any way that will disrupt their use for others in any way;
- I will not install or attempt to install or store programmes of any type on any School device, nor will I try to alter computer settings;
- I understand that I am not permitted to attempt to connect any devices or systems (e.g. laptops, mobile phones, USB devices, etc.) to any School devices, systems or services without prior permission from an Authorised Person within the School. I understand that, if I am permitted to use my own devices in the School I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the School's policies. I will not use my personal equipment to record these images, unless I have permission from the School and from the individual to do so;
- I will only use social networking sites in school in accordance with the School's policies;
- I will only communicate with students, parents / carers, and other parties solely related to my employment, using official School systems. Any such communication will be professional in tone and manner;
- I will not engage in any on-line activity that may compromise my professional responsibilities;
- I recognise that a failure to comply with the policies of the School, and any misuse of ICT equipment, could lead to breaches of the rights of data subjects and I will act at all times in accordance with such policies in order to avoid any inappropriate use of personal data, or the breach of the data protection rights of any individual.

I understand that I am responsible for my actions, both inside and outside of the School:

- I understand that the School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the School and where they involve my membership of the School community (for example, use of images, digital communications, or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the School ICT systems and services, disciplinary action as set out in the codes of conduct and in the event of illegal activities involvement of the police.

I agree to follow these guidelines at all times when:

- using or connected to the School's devices, systems and services;
- using my own equipment inside or outside of the School in a way that is related to me being a member of this School (for example, communicating with other members of the School, accessing School email, websites and services).

I have read and understand that use of the School IT systems and devices is governed by the full Acceptable Use Policy.

User Signature:

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the organisation's most recent Acceptable Use Agreement (AUA).

I agree to abide by the organisation's most recent Acceptable Use Agreement (AUA).

Signature …….…… Date ……

Full Name …….... (print)

Job title ……..

Shottermill Junior School