E-safety and Acceptable Use of ICT Policy

This policy applies to all pupils, visitors and staff of Abbot's Hill, including EYFS.

Introduction

Access to technology offers many positive advantages for learning and our wider lives but brings, with its many opportunities, risks. The school seeks to embrace the use of ICT to enhance teaching, learning and administration whilst recognising its duty to protect both pupils and the school from its inappropriate and harmful misuse.

E-safety

E-safety encompasses Internet technologies and electronic communications such as mobile phones and tablets as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

E-safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff, visitors and pupils
- Sound implementation of E-safety policy in both administration and across the curriculum
- Safe and secure Internet access including the effective management of a filter
- Education of everyone in our school community regarding safe practice
- Security of sensitive data and information
- Adherence to all Acceptable Use Agreements

This Policy relates to other policies including those for:

- Safeguarding and Child Protection
- ICT
- Anti-Bullying
- Staff Code of Conduct and Safer Working Practice

Also relevant are the following**:**

- Use of Personal Device Agreement
- Loan of Device Agreement
- Acceptable Use Agreements

E-safety Co-ordinators

The school has appointed a named person in each section of the school to co-ordinate E-safety

Prep School (including Nursery)	ICT Co-ordinator	Mrs B Stern
Senior School	Head of ICT	Mr C Wells

It is the role of the E-safety Co-ordinators to keep abreast of current issues and guidance.

All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-safety and know what to do in the event of misuse of technology by any member of the school community. Useful information can be found at:

- CEOP (Child Exploitation and Online Protection) www.ceop.police.uk
- Childnet International www.childnet.com
- UK Council for Child Internet Safety https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
- www.thinkuknow.co.uk
- www.disrespectnobody.co.uk
- www.saferinternet.org.uk
- www.internetmatters.org
- www.pshe-association.org.uk
- Educateagainsthate.com
- www/gov/uk/government/publications/the-use-of-social-media-for-online-radicalisation

If the necessity arises, any member of staff can make a referral regarding an E-safety issue.

If this is a Safeguarding concern they should talk to the Designated Safeguarding Lead: the Head of Pupil Progress and Welfare, Miss E Impett ext. 121 (01442 839121 / 07701 009325) or one of the Deputy Designated Safeguarding Leads (Deputy Head, Head of Prep, Assistant Head – Senior, Assistant Head – Prep, Nursery Manager or Headmistress).

Teaching children how to keep safe when using ICT in school and at home

- The Internet is an essential element for education, business and social interaction. The School has a duty to provide pupils with quality Internet access as part of their learning experience, to enhance their learning and as a necessary tool for staff and pupils.
- The School Internet access is designed for pupils' safe use and includes filtering appropriate to the age of pupils.
- Pupils are taught what is and what not acceptable use of the Internet is and given clear objectives.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The School ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as ChildLine or the CEOP report abuse button
- Schemes of Work, informed by the Building Learning Power initiative, build pupils' resilience so that they are able and comfortable to alert staff to unacceptable sites, inappropriate use of social media and threatening, intimidating or coercive behaviour online.
- All staff complete Prevent training and are alert to the vulnerabilities that lead to radicalisation. As a school we need to be vigilant to this and update keywords to our filtering as they emerge. Our responsibility leads beyond our school gates and training, appropriate to the pupils' needs is provided.

- Pupils are taught that bullying, including online, is against our Code of Conduct and that the responsibility to follow our Acceptable Use Agreements extends beyond the school grounds into all electronic communications.
- We offer guidance for parents and pupils, allowing them to update their knowledge and become confident and responsible users of the Internet.
- Digital leaders offer advice to pupils through assemblies, posters and discussion, therefore heightening awareness from a child's perspective

Managing Internet Access

- Access to the school network is made available via wired and wireless connections,
- Guest Internet access is available on a separate wireless network
- The security of the ICT network is reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are discussed with the Network Manager and outside agencies, as appropriate.
- Access will be restricted or suspended for users who misuse or abuse their Internet access.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation must comply with this policy and our Acceptable Use Agreements
- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoid the risk of personal profile information being revealed.
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. their line manager.
- Bulk emails should only be sent by the School Office
- Staff must not cc groups of parents

Social networking and personal publishing

The Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Pupils and staff are encouraged to be aware of the ease of uploading personal information and the impossibility of removing inappropriate material once it has been published.

- The school will block/filter access to social networking sites for pupils, and will only permit use of online tools for collective communication that have been specifically approved, such as Google Classroom
- Pupils are advised never to give out personal details of any kind which may identify them, the School or their location.
- Our Acceptable Use Agreements provide guidance on the responsible use of social media and how to respond to inappropriate use and should be followed by all staff, pupils and visitors.

Managing filtering

- The School's Internet connection is managed by a Smoothwall Unified Threat Management device. This device filters and logs all Internet traffic to all network users (Staff, pupils and guests).
- An individuals' computer and web use is subject to automated scrutiny which can be escalated to retrieval and analysis by the IT Manager and their team. Issues identified are escalated as necessary in line with normal management procedures.
- Two levels of web filter exist: staff and pupil/guest. Staff access is filtered based on a set of industry standards augmented with customised categories. Pupils and guests have a more restrictive set of categories applied. We ensure search engine settings are safe and enforce YouTube content restrictions. .
- The Network Manager will work with appropriate bodies to ensure systems to protect pupils are reviewed regularly and improved as necessary, and will report to the Senior Leadership Group (SLG) as required.
- The SLG will also ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- In addition, the school uses Impero software to impose and monitor text based Block/Detect policies for all of our users. A set of modifiable trigger words are automatically monitored by the software and their use results in an instant alert being sent to the Technical Support Team. Depending on the severity of the trigger condition, relevant staff members responsible for pastoral care or safeguarding are informed.
- The computers in ICT3, which are used by the Prep School, have Hector's World Safety Button™, an on-screen panic button, allowing children to instantly escape from situations they are not comfortable with.
- If pupils discover an unsuitable site, it must be reported to their teacher or the named E-safety Co-ordinator who will then inform the Network Manager. Staff should report unsuitable sites directly to the Network Manager.

Emerging Technologies

- We will continue to review all devices as to the appropriateness of these in school. Apple watches are not deemed suitable and are not allowed in school. Kindles, laptops and phones are deemed acceptable as long as they are used in accordance with this policy and our Acceptable Use Agreements.
- Personal safety and security when travelling to school independently is important and we recognise that such pupils will need access to their mobile phones to protect them.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Inappropriate use of any mobile networked device will result in suspension/restriction of mobile device usage on site, and further/wider sanctions may be enforced if appropriate.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the school's **Data Protection Policy**

ICT access

- All staff will be given the School's **E-safety and Acceptable Use of ICT Policy** and its importance explained.

- All staff and visitors must read and sign the **Acceptable Use Agreement** before using any school ICT resources, including access to the Internet
- Visitors are issued a slip informing them that the Internet is filtered and monitored for their protection and by using the network they agree to being monitored.
- Parents and pupils will be asked to sign and return an **Acceptable Use Agreement** annually.
- Staff will be asked to sign and Acceptable Use Agreement upon starting work at the school and whenever the policy is amended thereafter
- Everyone will be informed that Internet traffic is monitored and can be traced to the individual user.
- E-safety rules will be posted in all ICT suites and discussed with the pupils as a minimum at the start of each year.
- Everyone will be informed that computer, network and printer use is recorded and can be traced to the individual user.
- Parents' attention will be drawn to this policy.
- The School will take all reasonable precautions to ensure that users access only appropriate material. However, owing to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The School cannot accept liability for the material accessed, or any consequences of Internet access.
- Complaints of Internet misuse will be dealt with initially by the Deputy Head or the Head of Prep.
- The E-safety Committee will undertake an E-safety audit regularly to assess whether appropriate measures are in place.
- All staff, pupils and visitors will be aware that misuse of ICT access will result in suspension of or restrictions to their access.

Sanctions

- All staff, pupils and visitors will be aware that misuse of ICT access will result in suspension of or restrictions to their access. Personal devices used at inappropriate times (as detailed in Acceptable Use Agreements) will result in pupils having the device confiscated for 5 school days and being required to attend an after school detention.
- Misuse by staff will be treated in the same way as any other misconduct issue.

Mobile Phones

- The school accepts that parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety, particularly when travelling to and from school or school related activities.
- Mobile phones are not allowed within the Prep School. However, in exceptional circumstances the Head of Prep may give permission for a pupil to bring a mobile phone to school. Mobile phones are not allowed under any circumstances in EYFS.
- If pupils are given permission by their parents to bring phones to school, these must be labelled with their name and form/year group. Each Form Tutor will complete a class list of phone numbers and serial numbers at the start of each academic year. This should be updated if pupils change their phone or their number.
- The School accepts no responsibility for replacing lost or damaged mobile phones which are brought to school. Parents are advised to ensure their household insurance

provides appropriate cover for pupils' mobile phones. Lost and stolen mobile phones can be blocked by the network provider.

- Pupils in Years 7 and 8 must hand their mobile phone in to the Form Tutor at morning registration and collect it from Main Reception at 4.30
- Pupils in Years 9-11 may choose to look after their own mobile phones. Use of these phones is permitted only in the designated areas at the designated times
- Use of a mobile phone must not lead to late arrival at lessons or activities.
- At all other times, phones must be out of sight and switched off. Failure to adhere with this requirement will lead to the phone being confiscated for 5 school days and an after school detention will be given.
- Pupils should protect their phone numbers by only giving them to their friends. This can help protect a pupil's number from falling into the wrong hands and guard against the receipt of unwanted calls and messages.
- Pupils are strongly advised to use passwords/pin numbers to prevent unauthorised access to their phones. These must not be shared.
- Use of mobile phones must adhere at all times to this **E-Safety and Acceptable Use of ICT Policy**.

Designated areas/times for use of devices, including phones

Prep School
Mobile phones are not allowed within the Prep School, including EYFS. Devices such as Kindles may be used with the permission of the teacher.

Senior School
School issued devices (Chromebooks) and Kindles can be used in lessons when authorised by the teacher concerned.

Girls may use authorised devices and phones as follows:

In Common Rooms, the Common Room Garden or the Rose Garden and Library (silent mode only)

At the following times:

Years 7 & 8	Before Registration and after 4.45pm
Years 9 – 11	Before Registration, during Break and Lunch, after 4.45pm

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-safety of individuals and groups within the school:

Headmistress

- Takes overall responsibility for E-safety provision
- Is responsible for ensuring that staff receive suitable training to carry out their E-safety roles and to train other colleagues, as relevant
- Is aware of procedures to be followed in the event of a serious E-safety incident.

- Receives regular monitoring reports from the E-safety Committee and Network Manager

Bursar

- Ensures the school uses an approved, filtered Internet Service, which complies with current statutory requirements
- Ensures that there is a system in place to monitor and support staff who carry out internal E-safety procedures (e.g. network manager)
- Ensures data and data security systems are robust

E-safety Co-ordinators

- Take day to day responsibility for E-safety issues and have a leading role in establishing and reviewing the school E-safety policies / documents
- Promote an awareness and commitment to E-safeguarding throughout the school community
- Ensure that E-safety education is embedded across the curriculum
- Liaise with the schools' ICT technical staff
- Facilitate training and advice for all staff

Designated Safeguarding Lead

- Communicates regularly with the Senior Leadership Group and Safeguarding Committee to discuss current issues, review incident logs and filtering / change control logs
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident
- Maintains an up to date E-safety incident log
- Liaises with the relevant agencies
- Ensures that they regularly update their knowledge of E-safety issues and legislation, and are aware of the potential for serious child protection issues to arise from:
  - sharing of personal data
  - access to illegal / inappropriate materials
  - inappropriate on-line contact with adults / strangers
  - potential or actual incidents of grooming
  - cyber-bullying and use of social media
- Oversee the delivery of the E-safety element of the curriculum

Board of Governors

- Reviews the effectiveness of the policy as part of its safeguarding responsibilities. This will be overseen by the Board Nominated Safeguarding Lead as part of the termly review of Safeguarding.
- Supports the School in encouraging parents and the wider community to become engaged in E-safety activities

Network Manager

- Reports any E-safety related issues that arise, to the E-safety Co-ordinators.
- Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed

- Ensures that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date
- Ensures the security of the School's ICT system
- Ensures that access controls / encryption exist to protect personal and sensitive information held on school-owned devices
- Ensures the School's policy on web filtering is applied and updated on a regular basis
- Ensures that they are up to date with the School's **E-safety and Acceptable Use of ICT Policy** and relevant technical information in order to effectively carry out their E-safety role and to inform and update others as relevant
- Ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- Keeps up-to-date documentation on the School's E-security and technical procedures
- May inspect any ICT equipment owned or leased by the school at any time without prior notice

Data Manager

- Ensures that all data held on pupils on SchoolBase (the school's MIS) and Kindersoft (Nursery management system) have appropriate access controls in place and ensures that users follow appropriate access protocols

Teachers

- Embed E-safety issues in all aspects of the curriculum and other school activities
- Supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant)
- Ensure that pupils are fully aware of research skills and are fully aware of the legal issues relating to electronic content such as copyright laws

All staff (including temporary staff and volunteers)

- Promote the School's E-safety policies and guidance
- Read, understand, sign and adhere to the school staff **Acceptable Use Agreement**.
- Are aware of E-safety issues related to the use of mobile phones, cameras and hand held devices, monitor their use and implement current school policies with regard to these devices
- Report any suspected misuse or problem to the E-safety Co-ordinators or Designated Safeguarding Lead
- Maintain an awareness of current E-safety issues and guidance e.g. through CPD, E-safety talks, etc.
- Model safe, responsible and professional behaviours in their own use of technology
- Ensure that any digital communications with pupils are on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Pupils

- Read, understand, sign and adhere to the relevant **Acceptable Use Agreement** (NB: at Reception/ KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- Know and understand School policy on the use of mobile phones, digital cameras and hand held devices
- Know and understand School policy on the taking / use of images and on cyber-bullying
- Understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the School's **E-safety and Acceptable Use of ICT Policy** covers their actions out of school, if related to their membership of the school
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
- Help the school in the creation/ review of E-safety policies

Parents

- The School seeks to work closely with parents in promoting a culture of E-safety.
- The School will contact parents where concerns arise about pupils' online behaviour and we hope that parents will feel able to share concerns with the school.
- We recognise that not all parents feel confident about protecting pupils from online risks at home and we arrange, on a regular basis, information sessions to assist.

Issue Date: September 2016

Review Date: September 2017 or earlier if major change

Elizabeth Thomas .

Elizabeth Thomas

Headmistress

Use of Personal Device Agreement

Name (Please print)	Item(s)	Purchase Date	Serial number

By signing this form I understand and agree the following:

1. This equipment is solely for educational use when in school.
2. I am responsible for the safekeeping of the above equipment and any associated data contained on this equipment.
3. Use in the classroom is only with the teacher's permission and where it relates to the specific activity.
4. Year 5-9 pupils can bring in kindles or similar devices that have no Internet access at all.
5. Year 10 and 11 pupils can use devices with 3G; however, they should be switched onto flight mode unless specifically agreed by the teacher.
6. The Bluetooth function of the device must be switched off at all times and not be used to send images or files to other devices.
7. Devices should be fully charged at home and no chargers should be brought into school.
8. The School accepts no responsibility for replacing lost, stolen or damaged mobile phones. Any of these personal devices should be covered on your home insurance.
9. Devices can be only used in designated areas at designated times unless with a teacher's specific permission.
10. This agreement does not apply to school supplied devices, which are the subject of a separate agreement.

I have read the Pupil **Acceptable Use Agreement** and I understand that any breach of this will have disciplinary consequences which may include confiscation of the item.

Signature of pupil	Parent signature	Date

Use of School Issued Device Agreement

Name (Please print)	Item(s)	Issue Date	Serial number

By signing this form I understand and agree the following:

1. This equipment is solely for educational use
2. I am responsible for the safekeeping of this equipment and any associated data contained on this equipment
3. Use in the classroom is only with the teacher’s permission
4. Devices can be used at other times in designated areas and/or at designated times as outlined in the E-Safety and Acceptable use of ICT Policy
5. Devices should be fully charged at home before coming to school and no chargers should be brought into school as facilities for charging are available in school
6. If this device is lost, stolen or damaged, the School will replace it for me. The cost of this will be charged on the termly bill to my parents
7. I understand that this device is subject to remote monitoring at any time

I have read the Pupil **Acceptable Use Agreement** and I understand that any breach of this will have disciplinary consequences.

Signature of pupil	Parent signature	Date

ICT Acceptable Use Agreement: Reception – Year 6

The School has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others. This agreement should be signed by a parent for Reception/ Years 1 and 2 and by a parent and the pupil for Year 3-6.

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes. This will be monitored and made available to my teachers
- I will only use my class e-mail address or my own school e-mail address when e-mailing
- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe and ensure all my contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others' details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I may bring in my own device for reading from Year 5 in accordance with the **Use of Personal Device Agreement.** This cannot be a mobile phone.
- I will not bring in memory pens or CD's into school unless I have permission.
- I will ensure that my online activity, both in school and outside school in accordance with the law will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts

………

I have read and understood the Acceptable Use Agreement

I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Name **Form:**

Signature of pupil	Parent signature	Date

ICT Acceptable Use Agreement: Years 7 & 8

The School has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others. This Agreement applies to all school devices and devices brought into school including mobile phones.

- Chromebooks are issued to all girls in Years 7-11 (Year 7 from January 2018) These should be used in accordance with this **Acceptable Use Agreement.**

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes and appropriate to my education.

- I will not download or install software on any school device.

- I will only log on to the School network, other systems and resources with my own user name and password. I will follow the School's ICT security system and not reveal my passwords to anyone and change them regularly.

- I will only use my school e-mail address and ensure that all ICT communications with pupils, teachers or others is responsible and sensible

- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use

- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher

- I will not give out any personal information online such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher

- I understand that images or recordings made within school (including at clubs, school bus or when otherwise representing the school) may only be taken with the specific permission and knowledge of a member of staff and in accordance with our image authorization policy.

- I am aware that when I take images of pupils and/ or staff that I must only store and use these for school purposes and must never distribute these outside the school network without the permission of all parties involved.

- I will ensure that my online activity, both in school and outside school in accordance with the law will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts

- I will respect the privacy and ownership of others' work online at all times

- I will not attempt to bypass the Internet filtering system

- I will recognise and report inappropriate sites to a member of staff so that these sites can be blocked. This information must be passed directly to the Designated Safeguarding Lead

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers

- I will ensure that any online activity, both in School and outside School will not, in accordance with the law, bring the School into disrepute.

- I may bring in my own device for reading in accordance with the **Use of Personal Device Agreement.** This cannot be a mobile phone**.**

Mobile Devices

- My mobile phone will be handed in at registration and collected at the end of the day. It will be kept out of sight outside these times.

- I may use my mobile phone in one of the designated areas before and after school as long as it abides with the **Acceptable Use Agreement**

- My phone should be clearly marked with my name, form and year. Serial numbers should be updated when I change my mobile phone.

- My mobile device should be used in accordance with this **Acceptable Use Agreement** on the school bus and at all times when representing the school.

- The School accepts no responsibility for lost or stolen devices including mobile phones and parents are advised to ensure that household insurance policies provide appropriate cover for these items.

……………………………………………………………………………………………..

I have read and understood the Acceptable Use Agreement

I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Name: **Form:**

Signature of pupil	Parent signature	Date

ICT Acceptable Use Agreement: Years 9-11

The School has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others. This Agreement applies to all school devices and devices brought into school including mobile phones.

- The computer system is owned by the School and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.
- Chromebooks are issued to all girls in Years 7 – 11. These should be used in accordance with this Acceptable Use Agreement.
- The School's **Online and Acceptable Use of ICT Policy** has been drawn up to protect all parties - the pupils, the staff, visitors and the School.
- Pupils should sign a copy of the **Acceptable Use Policy** annually.
- Access must only be made via the authorised personal login and password, which must not be made available to any other person.
- Activity that threatens the integrity of the School ICT systems, or that attacks or corrupts other systems, is forbidden.
- Use of school computer systems and mobile devices will be monitored and recorded by any means at the school's disposal (including remote screen viewing, viewing users' e-mails, viewing Internet browsing history, viewing files in users' areas).
- Internet use should be appropriate to a pupil's education and sites and materials accessed must be appropriate to work in school.
- All users must not attempt to circumvent any filtering mechanisms. Deliberate attempts to visit unsuitable sites may result in suspension of Internet access.
- All users will recognise and report inappropriate sites to a member of staff so that these sites can be blocked. This information must be passed directly to the **Designated Safeguarding Lead**
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The School reserves the right to examine or delete any files that may be held on its computer system and to monitor correspondence and any Internet sites visited.
- Users are responsible for e-mail they send and for contacts made that may result in e-mail being received.
- Copyright of materials and intellectual property rights must be respected.
- The normal rules of social interaction apply to e-mail and others forms of digital media.
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.
- The remoteness of the recipients must not be used to excuse anti-social behaviour: harassment, intimidation and bullying behaviour.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Use of social networking sites, chat rooms and instant messaging is not permitted on the School networks, including the Guest Wi-Fi, except as explicitly authorised by the School.
- Responsible use of mobile internet devices is expected at all times within school and on school led trips.

- All users must ensure that any online activity, both in School and outside School will not, in accordance with the law, bring the School into disrepute.
- Images and recordings may only be taken within the school, or during school related outings and activities, with the specific permission and knowledge of a member of staff in accordance with our **Image Authorisation Policy**.
- No device under any circumstances should be brought into any examination room unless an approved device for use by the invigilator.

Mobile Devices for Pupils

- Mobile devices should be switched off and kept out of sight unless in designated areas and at designated times unless given permission of a teacher directly supervising them as long as their use abides with this **Acceptable Use Agreement**
- Mobile devices should be used in accordance with this Acceptable Use Agreement on the school buses and at all times when representing the school.
- Phones should be clearly marked with the name, form and year group of the owner. Serial numbers should be updated when girls change their mobile phones.
- The School accepts no responsibility for lost or stolen devices including mobile phones and parents are advised to ensure that household insurance policies provide appropriate cover for these items.

Mobile Devices for pupils visiting the nursery

- Mobile phones and personal devices are strictly prohibited in the Nursery with the exception of the staff room during staff breaks only.
- On arrival, switch off the mobile phone and hand to the Nursery Manager. It will be signed in and locked away securely.
- At the end of their visit, pupils may retrieve their phone and sign it out. They should remain switched off until they leave the Nursery grounds.

……

I have read and understood the Acceptable Use Agreement

I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Name **Form:**

Signature of pupil	Parent signature	Date

Acceptable Use Agreement
Visitors and Staff

This Agreement refers to any networked device and personal devices or mobile phones.

- The computer system is owned by the School and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.
- The School's E-safety and Acceptable Use of ICT Policy has been drawn up to protect all parties - the pupils, the staff, visitors and the School.
- Staff will be asked to sign an Acceptable Use Agreement upon starting work at the school and whenever the policy is amended thereafter annually.
- All visitors are required to accept the terms of this agreement before or upon arrival.
- Access must only be made via the authorised personal login and password, which must not be made available to any other person.
- Activity that threatens the integrity of the School ICT systems, or that attacks or corrupts other systems, is forbidden.
- Use of school computer systems and mobile devices will be monitored and recorded by any means at the school's disposal (including remote screen viewing, viewing users' e-mails, viewing Internet browsing history, viewing files in users' areas).
- Internet use should be appropriate to a pupil's education and sites and materials accessed must be appropriate to work in school.
- All users must not attempt to circumvent any filtering mechanisms. Deliberate attempts to visit unsuitable sites may result in suspension of Internet access.
- All users will recognise and report inappropriate sites to the Network Manager/E-Safety Co-ordinator so that these sites can be blocked. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The School reserves the right to examine or delete any files that may be held on its computer system and to monitor correspondence and any Internet sites visited.
- Users are responsible for e-mail they send and for contacts made that may result in e-mail being received.
- Copyright of materials and intellectual property rights must be respected.
- The normal rules of social interaction apply to e-mail and others forms of digital media.
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.
- The remoteness of the recipients must not be used to excuse anti-social behaviour: harassment, intimidation and bullying behaviour.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Responsible use of mobile Internet devices is expected at all times within school and on school led trips.
- All users must ensure that any online activity, both in school and outside school will not, in accordance with the law, bring the School into disrepute.
- Images and recordings may only be taken within the school, or during school related outings and activities, with the specific permission and knowledge of a member of staff in accordance with our Image Authorisation Policy.

- No device under any circumstances should be brought into any examination room unless an approved device for use by the invigilator.

Mobile Devices for Staff working in or visiting the Nursery

- Mobile phones and personal devices are strictly prohibited in the Nursery with the exception of the staff room during staff breaks only.
- On arrival, switch off the mobile phone and hand to the Nursery Manager. It will be signed in and locked away securely
- On breaks, staff may retrieve their phone and use in the staff room only. They should be signed back out and back in before returning to work
- At the end of their shift/visit, staff may retrieve their phone and sign it out. They should remain switched off until they leave the Nursery grounds.

Mobile Devices for Staff elsewhere on the school site

- Personal mobile phones or recording devices must never be used to take photos or videos of children or any other aspect of the school
- Staff may use devices or phones for their normal purposes when they are in an office, staff room or in other locations when they are out of sight of pupils (except Nursery – see above).
- They may be used during educational visits as appropriate to the circumstances.
- They may be used as a teaching aid appropriate to the curriculum and lesson plan in question; however, it is advisable to seek clarification with your line manager.
- In the event of an emergency, mobile phones can be used at any time.
- Personal mobile devices cannot be used in any way that breaches Safeguarding. This may include but is not limited to:-
  - Taking photos of pupils
  - Communicating socially with pupils
  - Collecting information on pupils
  - Telephone numbers should never be made available to pupils and staff should alert the SLG if this has happened.

Mobile devices for parents and visitors to the school except Nursery and Reception

- Personal mobile phones or recording devices must never be used to take photos or videos of children or any other aspect of the school in accordance with our Image Authorisation Policy
- Parents may use their phone for normal purposes when visiting the school; however, they should consider the appropriateness of where, when and how the phone is used in order to avoid disruption to the smooth running of the school

Mobile Devices for Parents/Guardians visiting the Nursery and Reception

- When dropping off or collecting a child in the Nursery or Reception, mobile phones and personal devices should be kept out of sight. They are strictly prohibited from taking photos/videos, taking or making calls or using any of the device’s other features.

Mobile Devices for Visitors to the Nursery

- All visitors to the Nursery will be asked to switch off and hand in their device before entering any of the children’s rooms. They will be locked away securely and signed in and out as appropriate. The device must remain switched off until leaving the Nursery grounds.

I have read and understood the Acceptable Use Agreement

Name ……………………………………………….

Signature	Date