Online Safety Policy

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

1. Introduction

1.1 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.

2. Online Safety

2.1 Online 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.

2.2 Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff, visitors and pupils
- Sound implementation of the Online 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

2.3 This Policy relates to other policies including those for:

- Safeguarding and Child Protection
- ICT
- Anti-Bullying
- Staff Code of Conduct and Safer Working Practice
- Privacy Notice
- Data Retention Policy
- Image Authorisation Policy
- Staff Use of Social Media Procedures

2.4 Also relevant are the following**:**

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

3. Online Safety Co-ordinators

3.1 The school has appointed a named person in each section of the school to co-ordinate Online Safety

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

3.2 It is the role of the Online Safety Co-ordinators to keep abreast of current issues and guidance.

3.3 All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of Online 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
- https://educateagainsthate.com/
- https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

3.4 If the necessity arises, any member of staff can make a referral regarding an Online Safety issue.

3.5 If this is a Safeguarding concern they should talk to the Designated Safeguarding Lead: the Director of Pastoral Care, 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).

4. 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 **ICT 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 and Digital Ambassadors offer advice to pupils through assemblies, posters and discussion, therefore heightening awareness from a child's perspective.

5. 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 ICT Network Manager and outside agencies, as appropriate.
- Access will be restricted or suspended for users who misuse or abuse their Internet access.

6. 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. Staff should never use their personal e-mail accounts for school business. This protects sensitive school and personal data.
- 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 with the exception of PE who may contact groups to inform them of changes to fixtures. These must be done via SchoolBase or ClarionCall.
- Staff must not cc groups of parents.
- Weekly Bulletins will be used rather than individual's emails where possible.

7. Social networking and personal publishing

7.1 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. Pupils should regard it as their responsibility to report any serious misuse of social networking websites of which they become aware. This may be done on a 'no-names' basis provided sufficient information is given to enable the school to take action.

- 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.
- The school's computer systems must not be used to establish web pages on social networking websites or other websites of a kind described above. Disciplinary action would be taken against anyone who breaks this rule.
- Complaints, gossip or rumour about the school or a member of the school community will be investigated. Where they relate to the use of websites the school reserves the right to use inspection software to view web pages. This right will only be exercised when considered by the Headmistress to be necessary and reasonable in the interests of welfare, and in each case a decision to view web pages will be balanced against the pupil's right to respect for private and family life.
- Pupils will be held personally responsible for all material they have placed on a website and for all material that appears on a website of which they are the host or account holder unless it is removed at the first opportunity after its appearance.
- Material of a threatening, bullying, racist or harassing nature, whether placed during or outside school time (including the holidays) will be treated as a serious breach of school discipline. So will abusive or defamatory material if it is directed at members of the school community.
- Pupils are advised never to give out personal details of any kind which may identify them, the school or their location.
- Our **ICT 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.

8. 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 individual's computer and web use is subject to automated scrutiny which can be escalated to retrieval and analysis by the ICT Network 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 ICT 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 ICT Network Manager. 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 Online Safety Co-ordinator who will then inform the ICT Network Manager. Staff should report unsuitable sites directly to the ICT Network Manager.

9. 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 **ICT 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.

10. Protecting personal data

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

11. ICT access

- All staff will be given the school's **Online Safety Policy** and its importance explained.
- All staff and visitors must read and sign the **ICT Acceptable Use Agreement** before using any school ICT resources, including access to the Internet.
- Visitors are informed 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 **ICT Acceptable Use Agreement** annually.
- Staff will be asked to sign an **ICT 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.
- Online Safety rules will be posted in all ICT suites and discussed with the pupils as a minimum at the start of each year.
- Everyone is informed that computer, network and printer use is recorded and can be traced to the individual user.
- Parents' attention will be drawn to the **Online Safety Policy** via the **ICT Acceptable Use Agreement**.
- 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 Director of Pastoral Care.

- The Online Safety Sub Committee (DPC, ICT Network Manager, Online Safety Co-ordinators) will undertake an Online Safety audit regularly to assess whether appropriate measures are in place.
- The Online Safety Committee will meet termly to discuss emerging issues with regards to keeping our pupils safe online.
- All staff, pupils and visitors will be aware that misuse of ICT access will result in suspension of or restrictions to their access.

12. Sanctions

- All staff, pupils and visitors will be aware that misuse of ICT access will result in suspension of or restrictions to their network access. Personal devices used at inappropriate times (as detailed in **ICT Acceptable Use Agreements**) will result in school sanctions such as internal suspension or external suspension if the rules are repeatedly broken (see **Behaviour Policy**), 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.

13. 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. They will be handed into Main School Reception on arrival and collected from there at the end of the day. Mobile phones are not allowed under any circumstances in EYFS.
- All pupil phones should be clearly labelled with the name of the pupil and their year group.
- 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.
- Before the hours of 8.15am and 4.30pm phone use is permitted only in the designated areas.
- Pupils in Years 7-9 must switch off their phone at 8.15am and hand it in to the Form Tutor at morning registration and collect it from the library at 4.30pm.
- Pupils in Years 10 &11 will lock their phone away in the designated locker at 8.15am. It will be opened at 4.30pm until 5pm.
- Uncollected phones will be locked away in the Main Reception.
- 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 **Online Safety Policy**.

14. Designated areas/times for use of devices, including phones

Prep School
14.1 Mobile phones are not allowed within the Prep School, including EYFS. Devices such as Kindles may be used with the permission of the teacher and completion of Use of Reading Device Agreement.

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

14.3 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 -11 Before Registration and after 4.30pm.

15. Roles and Responsibilities

15.1 The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school.

15.2 Headmistress

- Takes overall responsibility for Online Safety provision.
- Is responsible for ensuring that staff receive suitable training to carry out their Online Safety roles.
- Is aware of procedures to be followed in the event of a serious Online Safety incident.
- Receives regular monitoring reports from the Online Safety Committee and ICT Network Manager.

15.3 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 Online Safety procedures (e.g. ICT Network Manager).
- Ensures data and data security systems are robust.

15.4 Designated Safeguarding Lead

- Takes day to day responsibility for Online Safety issues and reports concerns appropriately in accordance with the Safeguarding and Child Protection Policy.
- 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 Online Safety incident.
- Maintains an up-to-date Online Safety incident log.
- Liaises with the relevant agencies.

- Ensures that they regularly update their knowledge of Online 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

15.5 Online Safety Co-ordinators

- Have a leading role in establishing and reviewing the school Online Safety policies / documents.
- Promote an awareness and commitment to Online Safety throughout the school community.
- Ensure that Online Safety education is embedded across the curriculum.
- Liaise with the schools' ICT technical staff.
- Facilitate training and advice for all staff.
- Oversee the delivery of the Online Safety element of the curriculum.

15.6 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 Online Safety activities.

15.7 ICT Network Manager

- Reports any Online Safety related issues that arise to the DSL.
- 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 **Online Safety Policy and** relevant technical information in order to effectively carry out their Online 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 cyber security and technical procedures.
- May inspect any ICT equipment owned or leased by the school at any time without prior notice.

15.8 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.

15.9 Teachers

- Embed Online 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.

15.10 All staff (including temporary staff and volunteers)

- Promote the school's Online Safety policies and guidance.
- Read, understand, sign and adhere to the school staff **ICT Acceptable Use Agreement**.
- Are aware of Online 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 Designated Safeguarding Lead.
- Maintain an awareness of current Online Safety issues and guidance e.g. through CPD, Online 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.

15.11 Pupils

- Read, understand, sign and adhere to the relevant **ICT 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 Online Safety practice when using digital technologies out of school and realise that the school's **Online Safety** and **ICT Acceptable Use Agreement** 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 Online Safety policies.

15.12 Parents

- The school seeks to work closely with parents in promoting a culture of Online 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: June 2019
Review Date: June 2020 or earlier if major change

Elizabeth Thomas
Headmistress

Appendix 1

Use of reading devices (e.g. Kindles)

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. Years 5-9 pupils can bring in reading devices that have no mobile data.
5. Years 9-11 pupils can use reading devices with mobile data; 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 **ICT 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

Appendix 2

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 Online Safety 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 under a warranty/insurance scheme, faults and repairs should be resolved through the third party provider.
7. If this device is not covered by a warranty or insurance, then repairs or replacements will be chargeable to my parents.
8. I understand that this device is subject to remote monitoring at any time.

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

Signature of pupil	Parent signature	Date

Appendix 3

ICT Acceptable Use Agreement 2018-19: 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. Pupils should sign a copy of the ICT Acceptable Use Agreement annually.

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes. All use is monitored and available to my teachers.
- I understand that the school's Online Safety Policy has been drawn up to protect all parties - the pupils, the staff, visitors and the school. It is available on the website and the Parent Portal.
- I will only use my school e-mail address when e-mailing from school.
- 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 or iPod.
- 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 is in accordance with the law. I 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 ICT 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. Network access will only be given to pupils that have signed this **ICT Acceptable Use Agreement**

Name **Form:**

Signature of pupil	Parent signature	Date

Appendix 4

ICT Acceptable Use Agreement 2019-20: Years 7-9

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. Pupils should sign a copy of the ICT Acceptable Use Agreement annually.

- The school's Online Safety Policy has been drawn up to protect all parties - the pupils, the staff, visitors and the school. It is available on the website and the Parent Portal.
- 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 the senior school. These should be used in accordance with this ICT Acceptable Use Agreement.
- 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.
- Users are responsible for e-mails 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 between 8.15 and 4.30 unless given permission of a teacher directly supervising them as long as their use abides with this **ICT Acceptable Use Agreement**.

- Mobile phones will be handed in to the Form Tutor at registration and collected from the library at 4.30pm.
- Mobile devices should be used in accordance with this **ICT Acceptable Use Agreement** on the school buses 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 ICT 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. Network access will only be given to pupils that have signed this ICT Acceptable Use Agreement

Name:

Signature of pupil	Parent signature	Date

Appendix 5

ICT Acceptable Use Agreement 2019-20: Years 10 &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. Pupils should sign a copy of the ICT Acceptable Use Agreement annually.

- The school's Online Safety Policy has been drawn up to protect all parties - the pupils, the staff, visitors and the school.
- 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 the senior school. These should be used in accordance with this **ICT Acceptable Use Agreement**.
- 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.
- 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 locked away in the designated place between 8.15am and 4.30pm unless given permission of a teacher directly supervising them as long as their use abides with this **ICT Acceptable Use Agreement.**
- Mobile devices should be used in accordance with this **ICT Acceptable Use Agreement** on the school buses 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.

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 ICT 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. Network access will only be given to pupils that have signed this ICT Acceptable Use Agreement

Name:

Signature of pupil	Parent signature	Date

Appendix 6

ICT Acceptable Use Agreement: Staff

Staff will be asked to sign an ICT Acceptable Use Agreement upon starting work at the school and whenever the policy is amended thereafter and annually.

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 visitors and staff to enhance their professional activities including teaching, research, administration and management.
- The school's **Online Safety Policy** has been drawn up to protect all parties - the pupils, the staff, visitors and the school.
- 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).
- The school reserves the right to examine or delete any files that may be held on its computer. Internet use should be appropriate to a pupil's education and sites and materials accessed must be appropriate to work in school.
- No users must 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 ICT Network Manager/Online Safety Co-ordinator so that these sites can be blocked.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials and intellectual property rights must be respected. Users are responsible for e-mail they send and for contacts made that may result in e-mail being received.
- 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.
- Users must ensure that any online activity, both in school and outside school (will not), is in accordance with the law, and does not 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.

- When working remotely and connecting to a school computer, users should ensure their work can't be overlooked. Also do not leave that computer unattended at any time.
- Users working remotely must ensure that personal devices used to access the school network are secured with the latest operating system updates and anti-virus software.
- Users should never copy school personal data onto any private removable media (e.g. USB stick, DVD, external hard drive), or any privately owned device such as mobile phones, tablets, laptops etc. Even if the device is encrypted.
- If you do need to transport personal data outside of the school in a digital format, it must be done so using an encrypted device belonging to the school.
- If you must transport school personal data in paper format, ensure it is transported securely, keep it out of sight and never leave it unattended. Once it has reached its destination, secure it again in a locked draw/filing cabinet. Never remove the master copy of any personal data controlled by the school.
- On school trips, data should be transported securely and kept securely by the trip leader. All data should be returned to school, shredded or returned to the relevant person for safe storage.
- Discussing personal data whilst on a telephone call (personal and school owned device) must be done in private and away from anyone who might be able to hear your conversation.
- Only the School's Google Apps for Education cloud based storage systems should be used for school files, no other online storage services should be used.

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).
- School phones should be taken on educational visits and upon your return; any photos that have been taken will be immediately downloaded onto the appropriate media server by the ICT Network Manager.
- 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.

Staff Protocol for use of Social Media

- School phones can be used to upload pictures and text onto school Social Media accounts but you must abide by the following protocol.
- No personal devices are to be used to take pictures of pupils. When taking photos, it is preferable to use group pictures.
- All staff uploading pictures on social media must be aware of girls and staff who have withdrawn consent for their photo to be used. An up-to-date list is available on the T-Drive or can be obtained from Marketing.
- Staff may “Like” or “Retweet” AHS photos but must not copy and paste to any other Social Media Account or personal device. Comments made should be of a professional nature.
- Images should be uploaded at the lowest resolution possible. (see IT department for advice)
- No photos will be uploaded of pupils swimming or in swimwear except by Marketing. Pupils in gymnastics or trampolining leotards must be edited and cropped.
- Live posting can be used on Social Media however locations should not be shared or tagged. The fixture/tournament/trip title can be used i.e. U15 Netball, National Lacrosse Tournament, Paris Art Trip.
- If an image of a pupil is used, the full name should not be published. Only the first name of pupils can be used online (The first name and first initial of the surname is acceptable if there are multiple pupils with the same first name in a year group).

Abbot’s Hill Social Media Accounts

The following accounts are live and are managed by separate departments. They are responsible for monitoring content and alerting SLG if unacceptable posts or comments are added. They are only permitted to use school devices upload pictures.
Owners of social media accounts can use their own device and text only updates.

AHS Facebook -Marketing
AHS Twitter - Marketing
AHS Instagram - Marketing
AHS LinkedIn - Marketing
AHS Nursery Facebook - Marketing/Nursery Manager
AHS Technology Twitter - ICT Network Manager
AHS Nursery Twitter - Marketing/Nursery Manager
AH Sport Twitter and Abbot’s Hill School Sport Facebook-Head of PE
AHS Instagram - Head of PE
AHS STEM- Stem Co-ordinator
Abbot’s Hill ICT Twitter- Head of ICT
Abbot’s Hill Holiday Activity Clubs- Director of Holiday Clubs

I have read and understood the ICT Acceptable Use Agreement

Name ……

Signature	Date

Appendix 7

ICT Acceptable Use Agreement: Visitors

This agreement refers to any device connected to the Abbot's Hill School network.

- The school's **Online Safety Policy** has been drawn up to protect all parties - pupils, staff, visitors and the school.
- Visitors are required to accept the terms of this agreement before or upon arrival and before Guest network access is given.
- Access must only be made via the authorised username 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 personal devices using any school network is monitored. Internet traffic is filtered and all activity is logged.
- Visitors must not attempt to circumvent any filtering mechanisms.
- Visitors must ensure that any online activity is in accordance with the law.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials and intellectual property rights must be respected.
- Internet sites and materials accessed must be appropriate to work in school.
- Attempts to visit unsuitable sites may result in suspension of internet access.
- Users will recognise and report inappropriate sites to the ICT Network Manager/Online Safety Co-ordinator so that these sites can be blocked.

Mobile devices for Parents or 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.

GDPR

Use of your personal data will be in accordance with the school's legitimate interests. To view our privacy policy in full, please visit this link:
https://www.abbotshill.herts.sch.uk/wp-content/uploads/2018/05/Privacy-Notice-including-Appendix-1.pdf

I have read and understood the Acceptable Use Agreement.

Name	
Company/Organisation	
Signature	Date

Appendix 8

Acceptable Use Agreement: School Governors

This Agreement refers to any networked device and personal devices or mobile phones. Governors will be asked to sign an Acceptable Use Agreement upon commencing service at the school and whenever the policy is amended thereafter annually.

- 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 **Online Safety Policy** has been drawn up to protect all parties - the pupils, the staff, visitors and the school.
- Access must only be made via the authorised guest 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 ICT Network Manager/Online 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**.
- If a personal or school provided device which has access to our network is lost or stolen, this must be reported to the ICT Department immediately. 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 School Governors 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
- Governors 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).
- 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.

I have read and understood the Acceptable Use Agreement

Name ……

Signature	Date