The Brook

Online Safety Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital information technologies are powerful tools, for learning. The children have an entitlement to use the internet and related communication technologies appropriately and safely at all times. This is part of the wider duty of care to which all who work in schools are bound.

This school online safety policy has been written to help to ensure safe and appropriate use.
The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote achievement.

However, the use of these new technologies can put children at risk within and outside the school. Some of the dangers they may face both now and as they grow older may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies i.e. Behaviour, Anti-bullying and Child protection policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build the children's resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

As a school we will provide the necessary safeguards to manage and reduce these risks. This online safety policy explains how we intend to do this, while also addressing wider educational issues in order to help children (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Schedule for Development and monitoring

This online safety policy was approved by the Board of Governors for The Brook School *:*	
The implementation of this online safety policy will be monitored by the:	*Online safety Group, Online safety Governor Sandy Tong, ICT Co-ordinator Mrs Ungless, ICT Technician Mrs Hill and School Headteacher Miss Dowley*
Monitoring will take place at regular intervals:	*Yearly*
The *Governing Body* will receive a report on the implementation of the online safety policy generated by the monitoring group	*Yearly*
The Online safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*June 2017*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*School Headteacher, Governing Body, LA Safeguarding Officer, Police*

Scope of the policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents, carers, and visitors) who have access to and are users of school ICT systems.
The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when

they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school , but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and responsibilities
Governors / Board of Directors:

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online safety Governor the role is currently held by Sandy Tong. The role of the Online safety Governor will include:

- regular meetings with the Online safety Co-ordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings

Headteacher and Senior Leaders – Miss Dowley, Miss Hack

- The Headteacher, Miss Dowley, is responsible for ensuring the safety (including online safety) for all members of the school community.
- The Headteacher is responsible for ensuring that the Online safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Senior Leadership Team will receive regular monitoring reports from the Online safety Co-ordinator / Group.
- The Headteacher and Deputy Headteacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. They will refer to the flow chart in Appendix A for dealing with online safety incidents "Responding to incidents of misuse" and relevant West Sussex disciplinary procedures for guidance.

Online safety Co-Ordinator – Anna Hill

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- receives reports of online safety incidents. meets regularly with Headteacher/Senior Leadership Team to discuss current issues, and review incident logs

ICT Technician – Anna Hill

- Ensure that the Acceptable Usage Policies and guidance is up to date.
- Keeps a record of all AUP staff acceptance forms.
- Ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- Usage Policy and any relevant Local Authority Online safety Policy and guidance that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Keeps a log of all eSafety incidents and provides a regular report to the eSafety Co-ordinator, Headteacher and Governors.
- Current filtering provider is informed of issues relating to the filtering
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher, or Deputy Head for investigation.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Online safety Co-Ordinator/ Headteacher / Deputy Head or Class teacher as appropriate for investigation
- digital communications with children (e.g. email / Virtual Learning Environment (VLE) / voice) should be on a professional level
- online safety issues are embedded in all aspects of the curriculum and other school activities
- children are supported to understand and follow the school online safety and acceptable use policy

- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites that they visit.

The Designated Person for Child Protection

- should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - potential or actual incidents of grooming
    - cyberbullying

Online safety Group

The Online safety Group provides a consultative group that endeavours to have a wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body. As The Brook is a smaller school this group is made up of the ICT Technician, ICT Coordinator, Head Teacher and School Administrator.

Members of the Online safety Group will assist the Online safety Coordinator with:

- the production / review / monitoring of the school online safety policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Children at this school

- will have the opportunity to be a part of the Student Council which will be involved in ICT policy and decisions
- are expected to use the school ICT systems in accordance with the Pupils Rules for Internet Use
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be supported to understand school policies on the use of computers, digital cameras, hand held devices and mobile phones at an appropriate level to their age and stage of development.
- should understand the importance of adopting good online safety practice when using digital technologies out of school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through providing relevant information, for example, information sessions, newsletters, website / VLE and information about national or local online safety campaigns*.*

Parents and carers will be responsible for

- signing the Children's Rules for Internet Use
- supporting the school by encouraging the same rules at home.
- accessing the school website / VLE in accordance with the relevant school Acceptable Use Policy.

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / pupils* in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- The Online safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- where children are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the children visit.
- children should be taught in all lessons to be critically aware of the materials / content they access on-line

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected where possible
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Use of digital and video images - Photographic, Video

- The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils' instant use of images that they have recorded themselves or downloaded from the internet.
- However, staff, parents and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
- When using digital images, staff should inform and educate children about the risks associated with the taking, using, sharing, publication and distribution of images. In particular they should begin to recognise the risks attached to publishing their own images on the internet.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and

publication of those images. Images should only be taken on school equipment. Personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children and families must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's full names will not be used anywhere on a website/VLE, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website, VLE or newspapers as part of the Acceptable Use Policy signed by parents or carers when children commence at the school.
- Children's work can only be published with the permission of their parents or carers.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the teacher and IT Technician
- School will ensure that the use of Internet derived materials by pupils and ensure that staff comply with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and to respect copyright when using material accessed on the Internet.

Email

- Access in school to external personal e-mail accounts may be blocked.
- All staff have access to a WSGfL email address for work correspondence but may, if they wish to do so, use their personal email address.

- All users must immediately report, to the ICT Co-Ordinator/Technician, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Emails sent to external organisations should be written carefully in the same way as a letter written on school headed paper.
- Any digital communication between staff and parents/carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- The forwarding of chain letters is not permitted.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- School staff should ensure that:
- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Filtering

A filtering system is provided and is in place via Atomwide.

Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Published Content and the School Web Site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

The Headteacher will take overall editorial responsibility and the school administrator will ensure that content is accurate and up to date.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website/VLE, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs/work of pupils is published on the school website/VLE.
- Written permission from parents/carers will be obtained before photographs/work of pupils is published in newspapers.
- Work can only be published with the permission of the parents/carers.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

Data Protection

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:
    - Fairly and lawfully processed
    - Processed for limited purposes
    - Adequate, relevant and not excessive
    - Accurate
    - Kept no longer than is necessary
    - Processed in accordance with the data subject's rights
    - Secure
    - Only transferred to others with adequate protection
- Staff must ensure that they:
    - At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
    - Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
    - Transfer data using encryption and secure password protected devices.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor West Sussex County Council can accept liability for the material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow the policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If any apparent or actual misuse appears to involve illegal activity the flow chart in Appendix A will be consulted and actions followed, in particular the sections on reporting the incident to the police and the preservation of evidence.

- Any complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse will be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the School online safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School online safety Policy in newsletters, the school prospectus and on the school website.

Pupil Rules for Internet Use

- Ask permission before using the Internet.
- Only use your own class or pupil network login and password.
- Do not bring your software or disks into school without permission.
- Do not ignore pop-up boxes you do not understand – Tell the Teacher.
- Only e-mail and open attachments from people you know, or your teacher has approved.
- Messages you send must be polite and sensible.
- Never give out your personal details; home address or phone number, or arrange to meet someone.
- If you see anything you are unhappy with or receive messages you do not like, you should tell a teacher immediately.
- The school may check your computer files, e-mails sent and the Internet sites visited.
- Deliberately breaking these rules may result in you not being allowed to use the Internet or computers.