Barncroft Primary School

E-Safety Policy

Document Information			
Policy Number:	POL-R-011	**Created by:**	HT
Reviewed by:	Resources	**Responsibility:**	Resources
Last Review:	March 2016	**Next Review:**	March 2017
Review Cycle:	Annual	**Ratified by FGB:**	N/A
Signature (Chair of Resources Cttee):			

Our school vision for Computing
To prepare children with the skills and knowledge needed to be active participants in an ever changing digital world.

1. THE LAW

a. As legislation is often amended and Regulations introduced, the references made in this Policy may be to legislation that has been superseded. For an up to date list of legislation applying to schools, please refer to the Department for Education website at www.education.gov.uk/schools

i. Computer Misuse Act 1990
ii. Data Protection Act 1998

2. WHO WILL WRITE AND REVIEW THE POLICY?

a. Our e–Safety Policy has been written by the school, using advice of HCC and government guidance. It has been agreed by the Senior Leadership Team and approved by governors. This e-Safety Policy is part of the School Development Plan and relates to other policies including Behaviour Policy, Child Protection Policy, Data Protection Policy and Health and Safety Policy.

3. MANAGEMENT

a. The Headteacher will:

i. Ensure that this e-Safety policy is implemented and compliance with the policy is monitored
ii. Appoint an e-Safety Coordinator and a Computing Coordinator.
iii. Appoint Hampshire IT (through the Hampshire School Service) to maintain and run the school network
iv. Ensure that Staff training in safe and responsible Internet use both professionally and personally will be provided as part of Safeguarding/Child Protection training
v. Authorise staff to send e-mails sent to external organisations on behalf of the school within the parameters of their roles and responsibilities
vi. Take overall responsibility for published content on the school's website
vii. Ensure immediate action is always taken to block reported inappropriate web sites
viii. Record all e–Safety complaints and incidents — including any actions taken
ix. Ensure that all reported incidents of cyber bullying are properly investigated in accordance with the Behaviour Policy and recorded in the Behaviour Log folder
x. Ensure that Web Filtering offered through Hampshire County Council is in effect.

b. The e-Safety Coordinator/Computing Coordinator will:

i. With the Senior Leadership Team, work in partnership with parents, the Local Authority and Department for Education to ensure systems to protect pupils are reviewed and improved
ii. Set up whole class or group email addresses for communication outside of the school for use by teachers
iii. Moderate personal publishing sites used by pupils (within the terms of this policy)
iv. Post the Acceptable Use Agreement in all networked rooms
v. Update advice on filtering systems and educational and leisure activities, that include responsible use of the Internet and e–Safety, made available on the school website.

c. Teachers and Teaching Assistants will:

i. Implement the Teaching and Learning section below
ii. Ensure that all points in this policy relating to staff and pupils are implemented.

d. The Business and Administration Manager will:
    i. Correctly maintain the school's Data Protection Registration with the Information Commissioner
    ii. Liaise with the network administrator/ HCC to ensure safety of electronic records

e. Hampshire IT (Hampshire School Service) will:

    i. Be the network administrator for the school network (administration and curriculum), which is used by staff and pupils for education and administration purposes.

4. TEACHING AND LEARNING

a. **Why is Internet use important?**

    i. The Internet is an essential element in 21st century life for education, business and social interaction
    ii. The school has a duty to provide pupils with quality Internet access as part of their learning experience
    iii. Internet use is part of the statutory curriculum and a necessary tool for learning
    iv. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security
    v. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions
    vi. Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

b. **How does Internet use benefit education? Benefits of using the Internet in education include:**

    i. Access to worldwide educational resources including museums and art galleries
    ii. Inclusion in the National Education Network which connects all UK schools
    iii. Inclusion in government initiatives
    iv. Educational and cultural exchanges between pupils worldwide
    v. Cultural, vocational, social and leisure use in libraries, clubs and at home
    vi. Access to experts in many fields for pupils and staff
    vii. Professional development for staff through access to national developments, educational materials and effective curriculum practice

viii. Collaboration across networks of schools, support services and professional associations
ix. Improved access to technical support including remote management of networks and automatic system updates
x. Exchange of curriculum and administration data with the Local Authority (LA) and Department for Education (DfE)
xi. Access to learning wherever and whenever convenient.

c. **How can Internet use enhance learning?**

i. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
ii. Internet access will be planned to enrich and extend learning activities.
iii. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
iv. The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
v. Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.
vi. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
vii. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
viii. The use of blogs, the school website, Google Apps, Espresso and My Maths will establish and maintain strong links with home and extend children's learning outside of the school day.

d. **How will pupils learn how to evaluate Internet content?**

i. Where practical, staff should view sites before use with children.
ii. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
iii. The evaluation of online materials is a part of teaching/learning in every subject.
iv. Teachers are to teach children to understand and abide by copyright law.
v. Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
vi. Pupils will be taught about internet safety.

5. SYSTEMS SECURITY AND MANAGING INTERNET ACCESS

a. The school is registered with the Information Commissioner under the Data Protection Act. The Business and Administration Manager is responsible for maintaining the registration.

b. The school maintains a hosted service as supplied through HSS. The hosted service will abide by HCC protocols and instructions:

   i. The Computing Co-ordinators are the main points of contact with HCC who are the network administrators under the HSS service agreement

c. The server is maintained and backed up by HSS, this is done automatically as part of the Hampshire Schools Service. This data is stored off site as per HCC guidelines.

d. **How will information systems security be maintained?**

   i. Internet access is regulated by HSS supplied filtered broad band connection which blocks access to unsuitable web sites.
   ii. The security of the school information systems and users will be reviewed regularly.
   iii. HSS supply antivirus software has been installed on the system and is maintained and kept up to date by this service
   iv. Staff passwords are changed regularly as prompted by the system. They are to contain both letters and numbers.
   v. Staff are required to adequately safeguard and, where possible, encrypt any personal or confidential data that is saved to laptops. If personal data has to be saved to other media, e.g. data sticks or CDs, it is to be encrypted or password protected.
   vi. Staff with access to the IT systems containing confidential and personal data are to ensure that such data is properly protected at all times. As a rule of thumb, where data is displayed on screen, either the room should be occupied by a member of staff, or the access points to the room secured. It is staff responsibility to ensure that their terminals are 'locked' (hence password protected) when the for mentioned terminals are left unattended or otherwise not logged off.
   vii. Personal or confidential data sent over the Internet or taken off site should be encrypted or password protected.
   viii. Portable media may not used by children without specific permission followed by a virus check.
   ix. Unapproved software will not be allowed on the school network or attached to email. Staff and pupils are not allowed to install their own software, unless otherwise authorised to do so by the Network Administrator (HSS) or Computing Co-ordinators.

x. The Computing Coordinator/Network Administrator will review system capacity regularly with HSS.

e. **How will email be managed?**

i. Pupils may only use approved email accounts on the school system.
ii. Pupils must immediately tell a teacher if they receive offensive email.
iii. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
iv. Whole class or group email addresses will be set up on request for educational use and used under the guidance/direction of class teachers
v. Social email use can interfere with learning and will be restricted.
vi. The Headteacher authorises staff to send e-mails sent to external organisations on behalf of the school within the parameters of their roles and responsibilities
vii. The forwarding of chain/spam messages is not permitted
viii. Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team.

f. **How will published content be managed?**

i. The contact details on the website should be the school address, email and telephone number.
ii. Staff or pupils' personal information must not be published.
iii. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

g. **Can pupil's images or work be published?**

i. Images that include pupils will be selected carefully and only used if a parent has agreed for such images to be posted online. Children will never be named in photos.
ii. Pupils' full names will not be used anywhere in the public domain, particularly in association with photographs.
iii. Written permission from parents or carers will be obtained before images of pupils are electronically published. This permission will be reviewed on an annual basis.
iv. Pupils work can be published without their permission.

h. **How will social networking, social media and personal publishing be managed?**

i. Pupils will not be allowed access to public or unregulated chat rooms. The filtered broadband will see that this happens
ii. Pupils will not access social networking sites for example 'Facebook' or 'Twitter'. Pupils should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.
iii. Pupils will be instructed never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, birthday, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
iv. Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
v. School and class blogs should be password protected and run from an approved site and with approval from the Senior Leadership Team. The Head teacher must be added as a contributor on all blogs.
vi. When selecting the name for a class blog, it is essential that a name is chosen that will not generate search results with obscene or unsuitable titles. Before settling on a name, extensive Google searches should be made using every combination of the words in the title, including possible mis-spellings together with the word 'blog' and 'blogging'. If any offensive words appear in the first page of the search results, the name should be abandoned. All requests for new blogs must go through the Headteacher.
vii. Staff will be instructed not to run social network spaces for pupil use on a personal basis.
viii. If personal publishing is to be used with pupils then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by the Computing Co-ordinator.
ix. Pupils will be advised on security and encouraged to set secure, difficult-to-guess 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 by making profiles private.
x. Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory. Any form of bullying or harassment is strictly forbidden in accordance with the school's Behaviour Policy

i. **How will filtering be managed?**

i. The Computing Co-ordinator with the Senior Leadership Team will work in partnership with parents, the Local Authority and Department of Education to ensure systems to protect pupils are reviewed and, where necessary, improved.
ii. The school's broadband access will include filtering appropriate to the age and maturity of pupils. Maintenance of the list of blocked sites is a major task as new sites appear every day. This is done centrally by Hampshire County Council.
iii. Whenever a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Headteacher, who will then in turn report it to HCC (through the Hampshire Schools Service) for central blocking. This can be done very quickly – inside an hour.
iv. If an adult finds a site that they consider unsuitable, they should report it to the Headteacher. If the Headteacher is not available, it should be reported to the Deputy Headteacher or Business and Administration Manager who will arrange for it to be blocked immediately.
v. It is important for staff and parents to realise that web filtering from HCC works on a categorisation system and is not able to filter out individual offensive words. This may, on rare occasions, result in offensive words appearing in the titles of some search results. It is incumbent upon us to ensure that we work carefully to help children search safely online.

j. **How can photographic, video and audio technology be managed?**

i. Children should never bring their own cameras into school for use, except when specifically arranged for the purposes of learning.
ii. Children must not use personal phones to take photographs. All phones must be taken to the office as soon as they arrive at school. Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed and suitably covered.
iii. It is never appropriate to use photographic or video devices in changing rooms or toilets unless for a specific reason and under close supervision.
iv. Staff may use photographic or video devices (including digital cameras and mobile phones) to support school trips and curriculum activities. They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher (e.g. class blogs), nor circulate them in electronic form outside of school.

v. Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken. It is important to observe copyright relating to images and video.
vi. Parents are able to take photos/ videos of their own children in class assemblies and school events with the clear understanding that they will not upload or otherwise distribute these images either for personal use or financial gain. There may be occasions when the school request that this activity does not take place due to licence restrictions imposed by third parties. For example licence restrictions on purchased materials.

k. **How can emerging technologies be managed?**

i. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
ii. Staff will be issued with a school phone where contact with pupils is required. In exceptional circumstances and with the express permission of the child's parent and the Headteacher, a teacher may, for a specific period of time and for a specific purpose, use their own phone. This will be a most unusual set of circumstances.
iii. Mobile phones will not be used during lessons or formal school time, except by prior agreement with the Headteacher and for a specific learning activity. The sending of abusive or inappropriate text, picture or video messages is forbidden.

l. **How should personal data be protected?**

i. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
ii. The school has a Data Protection Policy (POL-043), which must be adhered to.

6. POLICY DECISIONS

a. How will Internet access be authorised?

i. All staff and pupils will have access to the internet through the school's network.
ii. All staff must read and sign the Staff and Volunteer Acceptable Use Agreement. Volunteers who use the school's IT equipment must also sign this agreement
iii. It is expected that children in Years 3 through to 6 will sign the School's Pupil Acceptable Use Agreement. Parents of children in Reception to Year 2 will be asked to sign this form having discussed it with their child.
iv. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences resulting from Internet use.
v. The Headteacher will ensure that the e-Safety policy is implemented and compliance with the policy monitored.
vi. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
vii. E-safety resources will be made available on the school website by the webmaster and signposted to parents at least termly in the School Newsletter.

b. How will e–Safety complaints be handled?

i. Complaints of Internet misuse will be dealt with under the School's Complaints Procedure which is publicly available on the school website.
ii. Any complaint about staff misuse must be referred to the Headteacher. Complaints about the Headteacher must be addressed to the Chair of Governors.
iii. All e–Safety complaints and incidents will be recorded by the Headteacher— including any actions taken.
iv. Pupils and parents will be informed of the complaints procedure.
v. Parents and pupils will work in partnership with staff to resolve issues.
vi. The Headteacher will hold discussions with the HCC Child Protection Officer to establish procedures for handling potentially illegal issues.
vii. Any issues (including sanctions) involving staff will be dealt with in accordance with the Staff Discipline, Conduct and Grievance Policy, Child Protection Policy and any other school policies as appropriate.

c. **How is the Internet used across the community?**

i. All use of the school Internet connection by community and other organisations shall be in accordance with this policy.

d. **How will Cyber bullying be managed?**

i. Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's Behaviour Policy
ii. There are procedures in place to investigate incidents or allegations of cyber bullying and support anyone affected by it - see the Behaviour Policy. The Headteacher is to be informed of all incidents of cyber bullying reported to the school. They will recorded in the Behaviour Log.
iii. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence. Staff will keep a record of any such incidents in their Learning Mentor files and pass a note of concern to the Designated Safeguarding Lead. The Headteacher must be informed of all such incidents and allegations.
iv. The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if the child is over ten years of age.
v. Sanctions for those involved in cyber bullying may include:
    1. The bully will be asked to remove any material deemed to be inappropriate or offensive.
    2. A service provider may be contacted to remove content.
    3. Internet access may be suspended at school for the user for a period of time.
    4. Parent/carers may be informed.
vi. The Police will always be contacted if a criminal offence is suspected.

e. **How will Blogs, Google Apps and other learning environments be managed?**

i. Senior Leadership Team (SLT)and staff will monitor the usage of the Class Blogs and Google apps accounts by pupils and staff regularly in all areas at least annually, in particular message and communication tools and publishing facilities.
ii. Pupils/staff will be advised on acceptable conduct and use when using any digital platform. This will be done through reading and signing the relevant Acceptable Use Agreement.
iii. All blogs will contain a link to the school's Acceptable Use Agreements.

iv. All blogs will be public, but moderated, so that all comments and posts not submitted by an approved contributor (class teacher/ head teacher) will be read and approved before being published..
v. All users will be mindful of copyright issues and will only upload appropriate content onto the blogs and Google apps accounts.
vi. When users leave the school their account or rights to specific school areas and blogs/ Google apps accounts will be removed or suspended.
vii. Any concerns with content may be recorded by the e-Safety coordinator or Headteacher and dealt with the following ways:
    1. The user will be asked to remove any material deemed to be inappropriate or offensive.
    2. The material will be removed by the appropriate administrator if the user does not comply or if removal of this material cannot be undertaken within a timely manner.
    3. Access to the blog /Google apps accounts for the user may be suspended.
    4. The user will need to discuss the issues with a member of SLT before reinstatement.
    5. A pupil's parent/carer may be informed.
viii. A visitor may be invited onto the blog/ Google apps account by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
ix. Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

7. COMMUNICATING THIS POLICY

a. How will the policy be introduced to pupils?

i. All users will be informed through the Acceptable Use Agreements that network and Internet use will be monitored.
ii. E–Safety training will be incorporated into the curriculum and raise the awareness and importance of safe and responsible internet use.
iii. An e–Safety module will be included in the PSHE, Citizenship and/or Computing programmes covering both safe school and home use.
iv. e–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
v. Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.
vi. The Pupil Acceptable Use Agreement will be visibly on display in all classrooms and areas where connections are available by Class Teachers and the Computing Co-ordinator.

b. **How will the policy be discussed with staff?**

i. This e–Safety Policy will be provided to all members of staff by the Headteacher.
ii. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
iii. Staff that monitor IT use will be supervised by the Senior Leadership Team and will report any incidents to the Headteacher.
iv. Staff training in safe and responsible Internet use both professionally and personally will be provided as part of Safeguarding/Child Protection training, provided by the Headteacher/ Designated Safeguarding Lead (DSL).

c. **How will parents' support be enlisted?**

i. Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website.
ii. A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events e.g. parent evenings, sports days.
iii. Parents will be requested to sign an e–Safety/internet agreement as part of the Home School Agreement.
iv. Information and guidance for parents on e-safety: advice on filtering systems and educational and leisure activities that include responsible use of the Internet on e–Safety will be made available on the school website and will be updated as needed by the Computing Co-ordinator.
v. Interested parents will be referred to organisations listed in Appendix 1 "e–Safety Contacts and References."

APPENDIX 1

E-SAFETY CONTACTS AND REFERENCES

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Safeguards Service: *www.kenttrustweb.org.uk?safeguards*

Click Clever Click Safe Campaign: *http://clickcleverclicksafe.direct.gov.uk*

Cybermentors: *www.cybermentors.org.uk*

Digizen: *www.digizen.org.uk*

Internet Watch Foundation: *www.iwf.org.uk*

Kidsmart: *www.kidsmart.org.uk*

Teach Today: *http://en.teachtoday.eu*

Think U Know website: *www.thinkuknow.co.uk*

Virtual Global Taskforce — Report Abuse: *www.virtualglobaltaskforce.com*

APPENDIX 2

BLOGGING GUIDELINES

We are really excited to have our class blogs and to be able to share the story of our school year. Keeping our blogs a safe and secure place to work is very important. Through the use of blogs the children at Barncroft Primary School have the opportunity to develop their understanding of online safety and how to behave when publishing to the Internet.

We have a few simple guidelines that we need to keep to in order to make the most of our blogs:

- Children are to only use their first name when commenting.
- Parents who leave comments are asked to use their first name only so as not to identify their child. Or post comments as "Albert's Mum" or "Juliet's Grandfather".
- All posts will be checked by a teacher before they are published to the blog.
- All comments are moderated by the class teacher before they appear on the blog.
- Always be respectful of other people's work - be positive if you are going comment.
- No text talk - write in full sentences and read your comments back carefully before submitting.

Everyone at Barncroft Primary School must adhere to these guidelines.

If you have any more concerns about the security of the blog then please pop into the school and have a chat with Mr Pitt or Mrs O'Rourke.

APPENDIX 3

Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will use the school's computers and internet connection for school work only.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords safe.
- I will not bring files into school without permission or upload inappropriate material to my user area.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet or meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- I will not wilfully damage school equipment. I understand that if I do this I may be asked to pay for replacement equipment.

Parental Agreement *(required for every pupil)*

I have read and understand these rules and agree to them.

We have discussed the rules together and I am confident that my child understands them.

Signature .....Date .....

Full Name ..... (printed)

Pupil Agreement *(for children in Year 3 to Year 6)*

I have read and understood these rules and agree to them.

Signature .....Date .....

Full Name ..... (printed)

APPENDIX 4

Staff and Volunteer Acceptable Use Agreement

Background

This scope of this agreement is fully described in the schools E-Safety Policy. This agreement covers the use of digital technologies and platforms in school: i.e. email, Internet, Google Docs for Education (aka '*involve*'), network resources (including remote access), blogging systems, software, equipment and other digital systems used in connection with the school.

Agreement

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (This is currently: Office 365 for external email and '*Involve*' (Google Apps for Education) for internal email and communications).
- I will only use the approved school email, communication platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Computing Co-ordinator or the Headteacher.
- I will not download or install any software or resources as I understand that this could compromise the network and may not be adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will make every effort to ensure that connected devices (including USB flash drives) have been scanned to detect and eliminate the possibility of viruses prior to their use on the school network.
- I understand Staff may use photographic or video devices (including digital cameras and mobile phones) to support school trips and curriculum activities. I will not upload images to the internet unless specific arrangements have been agreed with the Head teacher (e.g. class blogs), nor circulate them in electronic form outside of school.

- I will use the school approved platforms in accordance with school protocols and as described in the school E-Safety Policy.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role in accordance with school and HCC guidelines.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will keep any 'loaned' (e.g. Teacher Laptops) equipment up-to-date, using the school's recommended anti-virus, firewall and other IT 'defence' systems. *This is done by ensuring that such devices are brought in and logged in for the day once every two weeks.*
- I will access school resources remotely (such as from home) only through the HSS (Hampshire Schools Service) approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location. See E-Safety Policy for further guidance.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will alert the school's named child protection officer / relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand that it is my responsibility to access '*involve'* (Google Apps for Education) on a regular basis to ensure that I am informed regarding the day-to-day business and procedures of the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Staff and Volunteer Acceptable Use Agreement: Agreement form

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; an *involve* (Google Docs for Education) account; be connected to the Internet; be able to use the school's IT resources and systems.

Signature .....Date .....

Full Name ..... (printed)

Job title .....

School .....

Authorised Signature (Headteacher)

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

For Office Use only

SIMS Generated username:

……

Users personal e-mail (to receive initial login details):

……

IMPORTANT NOTE: One copy is to be retained by member of staff | Second copy for school file