Barncroft Primary School

E-Policy

including E-safety Policy, Staff Social Media Policy

& Staff Acceptable Use of ICT

Document Information			
Policy Number:	POL-R-011	**Created by:**	HT
Reviewed by:	Resources	**Responsibility:**	FGB
Last Review:	April 2019	**Next Review:**	April 2020
Review Cycle:	Annual	**Ratified by FGB:**	April 2020
Signature (Resources Lead Governor):			

Introduction

This document comprises, and makes reference to, the following recommended policies from the Hampshire County Council Manual of Personnel Practice:

- E-safety Policy
- School Social Media Policy
- Staff Acceptable Use of ICT Policy

In the rare occurrence of a conflict between the above policies the 'School Social Media Policy' and/or 'Staff Acceptable Use of ICT' should take precedence.

E-safety Policy

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is often amended and Regulations introduced, the references made in this Policy may be to legislation that has been superseded.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 2018

2. WHO WILL WRITE AND REVIEW THE POLICY?

Our E–Safety Policy has been written by the school, using advice of Hampshire County Council (HCC) and government guidance. It has been agreed by the Senior Leadership Team and approved by governors. This E-Safety Policy 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 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 on CPOMS
   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 and laptop trollies.
   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.
   ii. Undertake all actions and responsibilities under the agreed SLA.

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 Bug Club 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 fore 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 their 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 (or on their behalf by third party contractors).
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 at any times on the school grounds or while on school trips. All phones must be taken to the office or handed to the class teacher 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 2018.
ii. The school has a Data Protection Policy, which must be adhered to.

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 Local Authority (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 be recorded on CPOMS
iii. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence. Staff will record any such incidents on to the internal safeguarding system, CPOMS. 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.

2. 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

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 blogging:

- 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 such 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 contact the school’s Computing Coordinator or equivalent member of staff.

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)

School Social Media Policy

(From HCC Manual of Personnel Practice July 2019 – V1.4.1)

1 Preamble

1.1 This document should be read in conjunction with information contained in the Model Policy on Staff Acceptable Use of ICT in the Manual of Personnel Practice and on the County Council's "E-safety in Hampshire" webpage at https://www.hants.gov.uk/socialcareandhealth/childrenandfamilies/safeguardingchildren/onlinesafety, together with the Council's "Guidance on using Social Media" and other related policy documents referred to at Appendix 1 below. Each school will wish to customise the document to match its own specific situation.

1.2 The policy has been developed having regard to guidance provided by the professional associations for teachers and school leaders, other recognised trade unions, and by ACAS. It sets out the rules and standards to be applied for use of the Internet and social media in Hampshire schools. It provides information and guidance for both professional and personal use and outlines the risks to users and schools, as well as the potential consequences of misuse of the Internet and social media.

1.3 Where staff have concerns about e-safety, these should be raised with the Headteacher. Advice can also be sought from professional associations and trade unions.

2 Introduction

2.1 It is recognised that social networking has the potential to play an important part in many aspects of school life, including teaching and learning, external communications and continuing professional development. This policy therefore encourages the responsible and professional use of the Internet and social media to support educational delivery and professional development.

2.2 The Internet provides an increasing range of social media tools that allow users to interact with each other. Whilst recognising the important benefits of these media for new opportunities for communication, this policy sets out the principles that school staff, governors and contractors are required to follow when using social media.

2.3 It is essential that pupils/students, parents and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of students and staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

3 Objectives

3.1 The primary objective of this policy is to set out the responsibilities of staff, governors and contractors at the school who use the Internet and social networking sites. It is also aimed at ensuring that the Internet and social media are utilised safely, lawfully and effectively for the successful and economic delivery of school-based services.

4 Scope

4.1 This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

4.2 The policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school. It is acknowledged that there is significant potential for the school to exploit the Internet and social media and that this can bring great advantages. The use of both the Internet and social media is therefore actively encouraged.

4.3 The policy applies to personal webspace such as social networking sites (for example Facebook, MySpace, Yapper), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

4.4 This policy provides a structured approach to using the Internet and social media and will ensure that it is effective, lawful and does not compromise the school's reputation, school information or computer systems/networks.

5 Risks

5.1 The school recognises the risks associated with use of the Internet and social media and regulates their use to ensure this does not damage the school, its staff and the people it serves. Principal amongst these risks are:

- cyber bullying by pupils/students;
- access to inappropriate material;
- offending behaviour toward staff members by other staff or pupils/students;
- other misuse by staff including inappropriate personal use;
- inappropriate behaviour, criticism and complaints from external sources;
- loss or theft of personal data;
- virus or other malware (malicious software) infection from infected sites;
- disclosure of confidential information;
- damage to the reputation of the school;
- social engineering attacks - i.e. the act of manipulating people into disclosing confidential material or carrying out certain actions;
- civil or criminal action relating to breaches of legislation;
- staff members openly identifying themselves as school personnel and making disparaging remarks about the school and/or its policies, about other staff members, pupils or other people associated with the school.

6 Applying the Policy

6.1 <u>Responsibilities of staff members</u>

6.1.1 The following principles apply to online participation and set out the standards of behaviour expected of staff members as representatives of the School.

6.1.2 The School has a duty to provide a safe working environment free from bullying and harassment. If a staff member uses any information and/or communications technology, including email and social networking sites, to make reference to people working at or for the School, or people receiving services from the School then any information posted must comply with all relevant professional Codes of Practice and the School's ICT Acceptable Use Policy.

6.2 Using the Internet and social media for approved school purposes

6.2.1 Staff must ensure that they use the Internet sensibly, responsibly and lawfully and that use of the Internet and social media does not compromise school information or computer systems and networks. They must ensure that their use will not adversely affect the school or its business, nor be damaging to the school's reputation and credibility or otherwise violate any school policies. In particular:

- the school's Internet connection is for business use and its use, and use of social networking, must only take place in line with the school's policies;
- when acting with approval on behalf of the school, under no circumstances may staff comment or contribute unless identifying themselves as school staff;
- personal email or social media accounts must never be used to conduct school business. Any accounts created for this purpose must link to a school email address. The only exception is the use of professional networks (such as LinkedIn), where it is acceptable to use an account linked to a personal email address in both a professional and personal capacity;
- staff members must report any safeguarding issues they become aware of;
- staff members must not cite or reference pupils/students/parents without approval;
- material published must not risk actions for defamation, or be of an illegal, sexual, discriminatory or offensive nature;
- material published must be truthful, objective, legal, decent and honest;
- material published must not breach copyright;
- any publication must comply with all of the requirements of the General Data Protection Regulations (GDPR) 2016 and the Data Protection Act 2018, and must not breach any common law duty of confidentiality, or any right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information;
- material published must not be for party political purposes or specific campaigning which in whole or part appears to affect public support for a political party;
- material published must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns;
- the tone of any publication must be respectful and professional at all times, and material must not be couched in an abusive, hateful, or otherwise disrespectful manner;
- publication must be in line with school policies;
- if used with pupils/students, staff must ensure that the site's rules and regulations allow the age group to have accounts and that the parents are informed of its use;
- staff members must not use the Internet or social media if doing so could pose a risk (e.g. financial or reputational) to the school, its staff or services or where they do not have the approval from the Senior Leadership Team.

6.3 Personal use of Internet and social media

6.3.1 The school's Internet connection is intended primarily for educational use. There is no right for staff to use the Internet for private use and access can be withdrawn at any time. Where staff members are permitted access via the school's Internet connection:

- the school is not liable for any financial or material loss to an individual user in accessing the Internet for personal use;
- staff wishing to spend significant time outside of their own normal working hours using the Internet – e.g. for study purposes must obtain prior approval;
- inappropriate or excessive use may result in disciplinary action and/or removal of Internet facilities;
- the school will monitor Internet and email use by electronic means, and staff cannot expect privacy when using the school's Internet facility;
- personal Internet search histories and the content of emails sent for personal use will be accessed by staff only according to the Council's Internet, Intranet and Email Monitoring Policy and School's disciplinary procedures, and only then when a legitimate concern has been raised by monitoring processes, legitimate concerns expressed by a colleague, or some other legitimate and objective complaint or incident;
- electronic correspondence will only be intercepted in exceptional circumstances.
- users are not permitted to access, display or download from Internet sites that hold offensive material. Offensive material includes, but is not restricted to, hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. The school is the final arbiter on what is or is not offensive material or what is or is not acceptable, permissible or excessive use of the Internet – staff concerned about this should refrain from using the Internet for private matters;
- due to the potential impact on school systems, the use of streaming media such as video (YouTube, BBC iPlayer, Vimeo etc.) or audio (internet radio, Spotify, Google Music etc.) should be kept to a minimum. Streaming should be limited to occasional short video/audio clips only. Staff members must not stream TV, films or continual broadcasts (e.g. sport, news, radio or playlists);
- due to the potential impact on school systems, the downloading of media for personal use such as video (YouTube, BBC iPlayer, Vimeo etc.) or audio (internet radio, Spotify, Google Music etc.) is not permitted;
- certain websites will be blocked, but it is a breach of this guide to access any of the following types of site:
  - pornography/Adult /mature content
  - gambling/betting/gaming
  - alcohol/Tobacco
  - illegal drugs
  - auction sites
  - violence/hate/racism
  - weapons
  - any site engaging in or encouraging illegal activity
  - illegal file-sharing sites
- staff members who accidentally or unintentionally access a site containing any prohibited content must leave the site immediately and inform the Senior Leadership Team. Genuine mistakes and accidents will not be treated as breach of this policy;
- staff members may not download software from any source without approval;
- staff members are not permitted to alter or tamper with their PC Internet settings for the purpose of bypassing or attempting to bypass filtering and monitoring procedures unless they have been given express permission to do so by the Headteacher;

- staff members must not communicate personal or confidential information via the Internet/Intranet for any purpose, unless expressly authorised to do so by their Senior Leadership Team;
- users must not create, download, upload or transmit any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- users must not create, download, upload or transmit any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material;
- users must not create, download, upload or transmit material that is designed or would be likely to annoy, harass, bully, inconvenience or cause anxiety to others;
- users must not create, download, upload or transmit any unsolicited commercial or bulk web mail, chain letters or advertisements;
- users must not download any digital media including music, images, photos and video that would be in breach of copyright or licensing arrangements, or where copyright or ownership cannot be determined;
- the use of file sharing services or software is prohibited for any purpose;
- the use of cloud storage e.g. Google Drive, Dropbox, SkyDrive, iCloud, is not permitted for the storage of sensitive personal data.

6.4 School reputation and confidentiality

6.4.1 The school recognises an employee's right to a private life. However the school must also ensure its reputation and confidentiality are protected. Therefore an employee using any ICT away from school, including email and social networking sites must:

- refrain from identifying themselves as working for the school in a way that could have the effect of bringing the school into disrepute
- not express a personal view as a school employee that the school would not want to be associated with
- notify the Senior Leadership Team immediately if they consider that content posted via any information and communications technology, including emails or social networking sites, conflicts with their role in the school
- not have any unauthorised contact or accept 'friend' requests through social media with any pupil/student under the age of 18 (or under age 19 where the school has such provision), (including former pupils/students and/or those who attend other schools) unless they are family members;
- exercise caution when having contact or accepting 'friend' requests through social media with parents so as not to compromise the school's reputation or school information;
- not allow interaction through information and communications technology, including emails or social networking sites, to damage relationships with work colleagues in the school and/or partner organisations, pupils/students or parents
- not disclose any data or information about the school, colleagues in the school and/or partner organisations, pupils/students or parents that could breach the General Data Protection Regulations (GDPR) 2016 and the Data Protection Act 2018
- not use the Internet or social media in or outside of work to bully or harass other staff or others

6.5 Personal Information

6.5.1 School staff must never give out personal details of others, such as home address and telephone numbers. Staff must handle all personal or sensitive information in line with the school's Data Protection Policies.

6.5.2 With the rise in identity theft and fraud, staff may wish to consider the amount of personal information that they display on personal profiles.

7 Cyber bullying and Harassment

7.1 The use of ICT in relation to Bullying and Harassment

7.1.1 This section should be read in conjunction with the guidance contained in "Cyber-bullying: Practical Advice for School Staff". Cyber Bullying and Cyber Harassment, like other forms of bullying and harassment, imply a relationship where an individual has some influence or advantage that is used improperly over another person or persons, where the victim(s) is subjected to a disadvantage or detriment, and where the behaviour is unwarranted and unwelcome to the victim. However, in this case the technological environment has meant that the acts of bullying and harassment now include the use of information and communications technology including email and social networking.

7.1.2 The school will consider it a potential disciplinary matter if users utilise any information and communications technology, including email and social networking sites, in such a way as to bully/harass others in the school or in partner organisations, or pupils/students or parents, whether this takes place during or outside of work. Staff members need to be aware that no matter what the privacy settings on their social media/networking site, inappropriate/derogatory information about a colleague in the school or partner organisations, pupils or parents, can find its way into the public domain even when not intended.

7.1.3 It should be noted that a person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment.

7.1.4 If a staff member receives any threats, abuse or harassment from members of the public through their use of social media then they must report such incidents using the school's procedures. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182).

7.2 Senior Leadership responsibility in relation to Bullying and Harassment

7.2.1 The school owes a duty to take reasonable steps to provide a safe working environment free from bullying and harassment.

7.2.2 For this reason, it is essential that the Senior Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or

personally offensive emails, phone calls or content on social networking sites such as Facebook, Twitter, or by any other means.

7.2.3 If a Senior Leader is made aware of such an allegation, the Senior Leadership Team should deal with it in the same way as any other incident of bullying or harassment in line with school policies, by investigating the allegations promptly and appropriately and providing the victim with appropriate support to demonstrate that the matter is being dealt with seriously.

7.2.4 Senior Leaders should encourage staff to preserve all evidence by not deleting emails, logging phone calls and taking screen-prints of websites. If the incident involves illegal content or contains threats of a physical or sexual nature, the Senior Leadership team should consider advising the employee that they should inform the police. In the event that such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else. Therefore, the evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it. In these circumstances the Police should be contacted immediately for advice.

8. Signature

8.1 It will be normal practice for staff to read and sign a declaration as outlined in Appendix 2, to confirm that they have had access to the School Social Media Policy and that they accept and will follow its terms.

8.2 Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware, that in certain instances, inappropriate use of Social Media may become a matter for police or social care investigations.

SharePoint Unique Identifier	HRDOCID-561776108-75764
Version and date of publication:	V1.4 July 2018 V 1.4.1 July 2019
Owner:	EPS

Appendix 1

Legal and Policy Framework

The School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional Codes of Conduct, including the following:

- Human Rights Act 1998
- Common law duty of confidentiality
- General Data Protection Regulations (GDPR) 2016 and Data Protection Act 2018, and
- Employment Practices Data Protection Code

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the General Data Protection Regulations (GDPR) 2016 and the Data Protection Act 2018
- Information divulged in the expectation of confidentiality
- School or County Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952, 1996 and 2013
- Copyright, Designs and Patents Act 1988.
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Equality Act 2010

Related Policies

The Social Media policy should be read in conjunction with other relevant school and County Council policies, procedures and Codes of Conduct including:

- County Council Guidance on using Social Media
- IT Policy on email and internet use
- IT acceptable usage standards
- ICT Acceptable Use Policy for Staff
- Internet and Intranet Monitoring Policy

- Cyber bullying: Practical Advice for School Staff
- Disciplinary Procedures
- Equalities Policy

Appendix 2

Staff Declaration

I have read and understand the School Social Media Policy and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that, in certain circumstances, inappropriate use of Social Media may become a matter for police or social care investigations. I understand that if I need any clarification regarding my use of Social Media, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: …….

DATE: …….

PRINT NAME: ……

Staff Acceptable Use of ICT Policy

(From HCC Manual of Personnel Practice, September 2015: HF2894857)

1.0 Introduction

1.1 This model policy has been developed on behalf of all Hampshire maintained schools. Whilst Governing Bodies are advised to develop their own policy through consultation with staff and staff representatives to reflect their own systems and arrangements in school, it is appreciated that maintained schools that use Hampshire ICT services will have broadly similar requirements and therefore could adopt this policy for their own use.

1.2 Schools that do not use Hampshire ICT Services are likely to need to adjust this policy to reflect the systems in place in their school.

1.3 This Policy should be read in conjunction with other relevant school and County Council policies, procedures and Codes of Conduct including:

- School Social Media Policy
- Information Security – Corporate Acceptable Use Policy
- E-mail, Internet and Intranet Monitoring Policy
- Cyber bullying: Practical Advice for School Staff
- Disciplinary Procedure

1.4 Schools are encouraged to ensure that staff are given sufficient training and knowledge to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role. Schools and their staff are encouraged to make use of the resources developed by Childnet (http://www.childnet.com). Advice can also be sought from professional associations and trade unions.

2.0 Application

2.1 This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

2.2 The policy applies in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software (including use of software such as SAP and SIMS), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer's work.

2.2 This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

3.0 Access

3.1 School staff will be provided with a log on where they are entitled to use the school ICT facilities and advised what hardware and software they are permitted to access, including access to the internet

and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities.

3.2 Where staff have been provided with a school email address to enable them to perform their role effectively, it would not normally be used to communicate with parents and pupils unless express permission has been provided. Where staff are able to access email outside of schools hours, the email facility should not routinely be used to undertake school business outside of normal office hours.

3.3 Access to certain software packages and systems (e.g HCC intranet; SAP (HR, finance and procurement system), SIMS, RAISE Online, FFT, school texting services) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

3.4 Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection.

3.5 Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the school's policy in relation to use of pictures, is followed.

3.6 If the school does not provide school mobile phones, staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in these emergency situations and a cost incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

3.7 No mobile telephones or similar devices, even those with hands free facilities should be used whilst driving on school business.

3.8 Whether school staff have access to the school telephone system for personal use will be confirmed by the school. Where such use is made of this facility, it must be done during break periods, must not be excessive and the school should require either the cost of the call or a donation to be made towards the cost of the call.

3.9 The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.

4.0 Communication with parents, pupils and governors

4.1 The school communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. School must indicate to staff if any other staff are permitted to make contact using the systems below:

4.1.1 School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or a home/school link staff. Normally teaching assistants

and lunchtime supervisory staff would need to seek approval from a member of the senior leadership team where they feel they need to make a telephone call to a parent.

4.1.2 Text System – All Teachers and Office staff. Where other staff need to send a text, this is normally approved by a member of the Senior Leadership Team.

4.1.3 Letters – Normally all teachers may send letters home, but they may be required to have these approved by the Year Leader/Head of Department before sending. Where office staff send letters home these will normally require approval by the School Business Manager/Administrative Officer.

4.1.4 Email – school email accounts should not be used for communication with parents unless approved by a member of the senior leadership team. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

4.1.5 Visits home – All home visits are normally subject to approval by the senior leadership team and must follow the school's policy on home visits.

4.2 Under normal circumstances, school staff should not be using any of the methods outlined above to communicate directly with pupils. If a member of staff needs to contact a pupil direct via any of these methods, this must be approved by the Headteacher.

4.3 Where pupils are submitting work electronically to school staff, this must be undertaken using school systems and not via personal email.

5.0 Social Media

5.1 School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children. Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

5.2 Staff should refer to the School Social Media Policy which contains detailed advice on the expectations of staff when using social media.

6.0 Unacceptable Use

6.1 Appendix 1 provides a list of Do's and Don'ts for school staff to enable them to protect themselves from inappropriate use of ICT resources and equipment. School systems and resources must not be used under any circumstances for the following purposes:

6.1.1 to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share;

6.1.2 to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others;

6.1.3 to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material;

6.1.4 to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally;

6.1.5 to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils;

6.1.6 to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

6.1.7 to collect or store personal information about others without direct reference to The Data Protection Act;

6.1.8 To use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project;

6.1.9 to visit or use any online messaging service, social networking site, chat site, web-based email or discussion forum not supplied or authorised by the school;

6.1.10 to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people;

6.2 Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or ICT lead if applicable.

6.3 Where an individual accidently or unintentionally accesses a website or material that contains any prohibited content, they must leave the site immediately and inform the Headteacher or other member of the senior leadership team. Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team equally applies where school staff are using school equipment or facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated as a breach of this policy.

6.4 Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to the Headteacher or another member of the senior leadership team so that this can be dealt with appropriately.

7.0 Personal and private use

7.1 All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

7.1.1 taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)

7.1.2 interfering with the individual's work

7.1.3 relating to a personal business interest

7.1.4 involving the use of news groups, chat lines or similar social networking services

7.1.5 at a cost to the school

7.1.6 detrimental to the education or welfare of pupils at the school

7.2 Excessive personal use of school facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the member of staff.

7.3 It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, can have implications for their employment situation where this becomes known and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people.

7.4 Where school staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into the school, these personal items, should not be used during pupil contact sessions unless authorised. Staff should follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable staff to undertake their role but where it is used, staff should take care to ensure any school data/images are deleted following use of the equipment.

7.5 Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care and seek reimbursement as outlined in section 3.

8.0 Security and confidentiality

8.1 Any concerns about the security of the ICT system should be raised with a member of the senior leadership team.

8.2 Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.

8.3 School staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. Where staff are provided with a memory pen for such activity, to both protect the integrity of the server and to save space, this should be used. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to the school's ICT lead.

8.4 Where staff are permitted to work on material at home and bring it in to upload to the school server through their memory pens, they must ensure that they have undertaken appropriate virus checking on their systems. Where provided, staff should normally use their school issued laptop for such work.

8.5 Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil ICT system and/or VLE.

8.6 Whilst any members of school staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.

8.7 The school will nominate staff who are responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licences are maintained on all school based and school issued equipment. Staff must ensure that they notify the nominated staff when reporting any concerns regarding potential viruses, inappropriate software or licences.

8.8 Staff must ensure that their use of the school's ICT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, either through password protection on memory pens or through encrypted memory pens. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

8.9 Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

9.0 Monitoring

9.1 The school uses Hampshire County Council's ICT services and therefore is required to comply with their email, internet and intranet policies.

9.2 The school and county council reserve the right to monitor the use of email, internet and intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

9.2.1 to ensure that the security of the school and county council's hardware, software, networks and systems are not compromised

9.2.2 to prevent or detect crime or unauthorised use of the school or county council's hardware, software, networks or systems

9.2.3 to gain access to communications where necessary where a user is absent from work

9.3 Where staff have access to the internet during the course of their work, it is important for them to be aware that the school or county council may track the history of the internet sites that have been visited.

9.4 To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Chair of Governors, after discussions with relevant staff in Hampshire County Council's HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

10.0 Whistleblowing and cyberbullying

10.1 Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Headteacher to such abuse. Where a concern relates to the Headteacher, this should be disclosed

to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

10.2 It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their Headteacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182) and also via the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772.

10.3 Further advice on cyberbullying and harassment can be found in the School Social Media Policy and in Cyber bullying: Practical Advice for School Staff.

11.0 Signature

11.1 It will be normal practice for staff to read and sign a declaration as outlined in Appendix 2, to confirm that they have had access to the acceptable use policy and that they accept and will follow its terms.

11.2 Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware, that in certain instances, inappropriate use of ICT may become a matter for police or social care investigations.

APPENDIX 1

Do's and Don'ts: Advice for Staff

Whilst the wide range of ICT systems and resources available to staff, both in school and outside of school, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of school.

This Dos and Don'ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General issues

Do

- ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources
- ensure that where a password is required for access to a system, that it is not inappropriately disclosed
- respect copyright and intellectual property rights
- ensure that you have approval for any personal use of the school's ICT resources and facilities
- be aware that the school's systems will be monitored and recorded to ensure policy compliance
- ensure you comply with the requirements of the Data Protection Act when using personal data
- seek approval before taking personal data off of the school site
- ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely
- report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Headteacher or designated manager and/or Designated Safeguarding Lead as appropriate
- be aware that a breach of your school's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal
- ensure that any equipment provided for use at home is not accessed by anyone not approved to use it
- ensure that you have received adequate training in ICT
- ensure that your use of ICT bears due regard to your personal health and safety and that of others
- Don't
- access or use any systems, resources or equipment without being sure that you have permission to do so
- access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for
- compromise any confidentiality requirements in relation to material and resources accessed through ICT systems
- use systems, resources or equipment for personal use without having approval to do so
- use other people's log on and password details to access school systems and resources
- download, upload or install any hardware or software without approval
- use unsecure removable storage devices to store personal data
- use school systems for personal financial gain, gambling, political activity or advertising
- communicate with parents and pupils outside normal working hours unless absolutely necessary

Use of email, the internet, VLEs and school and HCC intranets

Do

- alert your Headteacher or designated manager if you receive inappropriate content via email
- be aware that the school's email system will be monitored and recorded to ensure policy compliance
- ensure that your email communications are compatible with your professional role
- give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate
- be aware that the school may intercept emails where it believes that there is inappropriate use
- seek support to block spam
- alert your Headteacher or designated manager if you accidentally access a website with inappropriate content
- be aware that a website log is recorded by the school and will be monitored to ensure policy compliance
- answer email messages from pupils and parents within your directed time
- mark personal emails by typing 'Personal/Private' within the subject header line

Don't

- send via email or download from email, any inappropriate content
- send messages that could be misinterpreted or misunderstood
- use personal email addresses to communicate with pupils or parents
- send messages in the heat of the moment
- send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude
- use email systems to communicate with parents or pupils unless approved to do so
- download attachments from emails without being sure of the security and content of the attachment
- forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention
- access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet
- upload any material onto the school website that doesn't meet style requirements and without approval

Use of telephones, mobile telephones and instant messaging

Do

- ensure that your communications are compatible with your professional role
- ensure that you comply with your school's policy on use of personal mobile telephones
- ensure that you reimburse your school for personal telephone calls as required
- use school mobile telephones when on educational visits

Don't

- send messages that could be misinterpreted or misunderstood
- excessively use the school's telephone system for personal calls
- use personal or school mobile telephones when driving
- use the camera function on personal or school mobile telephones to take images of colleagues, pupils or of the school

Use of cameras and recording equipment

Do

- ensure that material recorded is for educational purposes only
- ensure that where recording equipment is to be used, approval has been given to do so
- ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy
- ensure that parental consent has been given before you take pictures of school pupils

Don't

- bring personal recording equipment into school without the prior approval of the Headteacher
- inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded
- put material onto the VLE, school intranet or intranet without prior agreement from a member of senior staff

Use of social networking sites

Do

- ensure that you understand how any site you use operates and therefore the risks associated with using the site
- familiarise yourself with the processes for reporting misuse of the site
- consider carefully who you accept as friends on a social networking site
- report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site
- take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain
- ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page
- follow school procedures for contacting parents and/or pupils
- only contact pupils and/or parents via school based computer systems
- through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role)

Don't

- spend excessive time utilising social networking sites while at work
- accept friendship requests from pupils – you may be giving them access to personal information, and allowing them to contact you inappropriately
- put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial
- post anything that may be interpreted as slanderous towards colleagues, pupils or parents
- use social networking sites to contact parents and/or pupils

APPENDIX 2 : Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct. Staff should consult the detail of the school's Policy for Staff Acceptable Use of ICT for further information and clarification.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted.
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that school information systems and hardware may not be used for personal or private use without the permission of the Headteacher.
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance.
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication.
- I understand that I must not use the school ICT system to access inappropriate content.
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will follow the school's policy in respect of downloading and uploading of information and material.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher.

- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites.
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and where activities undertaken are inconsistent with expectations of staff working with children.
- I understand that it is my responsibility to access '*involve'* (Google Suite for Education) on a regular basis to ensure that I am informed regarding the day-to-day business and procedures of the school.

The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

I have read and understand the Policy for Staff Acceptable Use of ICT and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: ……

DATE:……..….

NAME (PRINT): ……