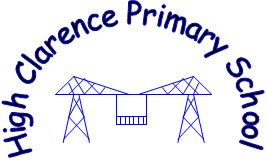
HIGH CLARENCE PRIMARY SCHOOL



Computing & E-Safety

Policy

October 2022

To be reviewed October 2023

**High Clarence Primary School Computing & E-Safety Policy**

Nicola Caraher – STEM Subject Leader

\*This policy should be read in conjunction with KCSIE September, Child Protection Policy, PSHE Policy, Anti-Bullying and Behaviour Policy, GDPR Policy and Child on Child Abuse Policy.

**Rationale**

Technologies encompass every part of modern life and it is important that our children are taught how to use these tools and more importantly, how to use them safely. We believe that it is important for children, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent independent users and learners of digital technologies we aim:

* To use digital technologies where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
* To use digital technologies to help improve standards in all subjects across the curriculum
* To develop the digital technologies competencies and skills of pupils through computing lessons and provide them with the chance to consolidate these in a cross-curricular context
* To ensure pupils are challenged in their use of digital technologies and are provided with exciting, creative ways in which to share their learning
* To use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation
* To provide all staff with the training and support to ensure that they can, and have the confidence to, use digital technologies, ICT and Computing to its full potential in all aspects of school life
* To use digital technologies as a form of communication with parents, pupils and the wider community

**Aims**

The school’s aims are to:

* provide a relevant, challenging and enjoyable curriculum for e-learning for all children.
* meet the requirements of the National Curriculum Programmes of Study for Computing.
* use digital technologies as a means to enhance learning throughout the curriculum
* respond to new developments in technology.

**Computing Curriculum**

Computing will be taught as a discrete curriculum subject according to the guidance in the National Curriculum for KS1 and KS2. There will be a need for the pupils to be taught stand-alone computing lessons but opportunities for developing computing across the curriculum should also be developed. The computing curriculum is split into three areas:

1. Digital Literacy

2. Computer Science

3. Information Technology

Pupils in EY, Key Stages 1 and 2 are taught Computing following school’s Computing curriculum. This ensures progression in the development of Computing techniques and capability.

The STEM Subject Leader will ensure that the plans provide coverage of what is expected through the new National Curriculum and Early Learning Goals. They will also ensure that the children are challenged and are able to succeed.

Opportunities for Computing across the curriculum should also be promoted at all levels across the school. Digital technologies are fundamental to children’s learning in our society they should be used when relevant in all curriculum subjects.

**Pupil Objectives for Computing**

**Early Years**

In Early Years they lay the foundations of computing. There is a clear link between the early years curriculum and the curriculum in KS1. In computer science, they develop knowledge and vocabulary of sequencing first, next and then. Technology is used to enhance, extend, model and develop learning. Opportunities are provided for the children to explore their immediate environment, living things, the world around them and people who are important to them and the use of technology plays an integral part. Children have access to a variety of ICT equipment, software and technology. These include computers, laptops, Interactive Whiteboards, iPads, CD players, metal detectors, cameras, scales, calculators and robots. As the children progress through EY they are provided with experiences to enable them to become independent with some equipment, to use it safely and to use pretend versions with purpose in their play. Technology is immersed in role-play through the use of equipment such as tills, scales, phones and microwaves.

Technology also supports early communication and language. It can offer new learning opportunities, through ebooks, apps, and even video calling. We believe, just like a book, technology is used as a tool for learning and play, rather than as a replacement for adult interaction. Through our holistic approach, technology provides our children with an additional resource to support learning. It also supports in developing children's gross motor skills, keyboard skills and hand-eye coordination.

The school follows the statutory National Curriculum for Computing. These statutory objectives relate to Key Stages 1 and 2.

**At the end of KS1 children should:**

* understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following precise and unambiguous instructions
* create and debug simple programs
* use logical reasoning to predict the behaviour of simple programs
* use technology purposefully to create, organise, store, manipulate and retrieve digital content
* recognise common uses of information technology beyond school
* use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

**At the end of KS2 children should:**

* design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts
* use sequence, selection, and repetition in programs; work with variables and various forms of input and output
* use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs
* understand computer networks, including the internet; how they can provide multiple services, such as the World Wide Web, and the opportunities they offer for communication and collaboration
* use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
* select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
* use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

**Assessment**

* Computer assessment is in line with the school’s Assessment Policy.
* Teachers are expected to make on going informal assessments in order to identify children who are constantly improving their capability and to help develop the skills and techniques of those who are not making the expected progress. The assessment of Computing also informs future opportunities for teaching and learning.
* The assessment of Computing should consider computing capability, consisting of knowledge, skills and understanding.

**Special Educational Need and Disability (SEND), More Able and Talented**

* All children will be given full access to the use of Computing in accordance with statutory requirements and the schools SEND Core offer.
* Differentiated Computing assistive technologies can succeed in removing barriers to learning, whilst helping children of all abilities, including those with SEN, reach their full potential.
* In planning lessons, teachers identify differentiated learning goals for a range of pupil groups, including SEND and More Able and Talented and identify appropriate Computing resources to enable those target groups to extend their learning and achieve their full potential.

**Equal Opportunities**

* All children regardless of gender, race, English as an additional language, social or economic background, ability or SEND are granted access to the use of all Computing equipment in order to develop their skills
* Steps will be made to explore that those children without home internet access will be given the opportunity to use the school facilities out of school hours – this could be during lunch, break times and after school.

**Multicultural Education**

At High Clarence we aim to ensure that Multicultural Education is included throughout the curriculum with relevant areas of study. Each subject leader provided opportunities for multicultural aspects to be explored within their subject and teachers include these in their medium term planning. These opportunities provide the children with resources and information that reflect the nature of society. They will have had the opportunity to further develop the children’s understanding and knowledge through focused activities linked to all areas of the curriculum.

**Monitoring and Review**

* The monitoring of the standards of the children’s work and of the quality of teaching and learning in Computing is the responsibility of both the senior leadership team and Computing subject leader.
* The Computing subject leader is also responsible for supporting colleagues in their teaching of Computing, for keeping them informed about current developments in the subject, and for providing a strategic lead and direction for Computing in school.
* All subject leaders and staff should take responsibility to ensure that the delivery of Computing is enriching, creative and stimulating. As computing plays a key role across the curriculum, individual subject leaders ought to ensure that they are engaging with current and emerging technologies.

**Internet, Systems and Services**

**Access and Deployment**

IT network infrastructure and equipment has been sited so that;

* Each classroom has a laptop connected to the network and a touch screen board.
* In KS2 classrooms our aim is that every child has their own iPad.
* There is a computer suite so children can access a computer individually during whole class Computing time.
* Nursery and Reception also have laptops in the classroom.
* Other equipment such as iPads

**Online Learning**

As a school, we value the importance of providing opportunities for children to learn outside of school and we will provide these depending on the age of the child.

Through a variety of programs such as Numbots, Times Table Rockstars, Education City, Espresso etc. Children are provided with their own individual logins and passwords. All children and families have access to SeeSaw, our platform encourages creativity and feedback that makes students excited to learn. Now more than ever, remote learning solutions are essential. Seesaw enables meaningful learning from anywhere, for every student.

**Resources**

The school acknowledges the need to continually maintain, update and develop its digital resources and to make progress towards a consistent, compatible IT system by:

• Maintaining a computer system to deliver a relevant and diverse curriculum

• Investing in software and hardware that will effectively deliver the strands of the Computing curriculum

• Investing in software that will support the use of ICT across the curriculum

Investing in infrastructure and equipment to improve children’s access to ICT across the curriculum and which also keep up to date with latest developments in technology.

**Resource Management**

High Clarence Primary is committed to reviewing the position and use of digital resources. The school will ensure the efficient deployment of existing digital resources and develop strategies for their replacement and for further purchasing to meet future needs.

**Equipment, Hardware and Software**

Hardware should not be installed without the permission of the Computing lead or Headteacher. If staff intend to use memory sticks which include sensitive information including (and not limited to) children’s names then they must use an encrypted memory stick. If staff use memory sticks to store other non-sensitive data then the school’s antivirus software will scan these. Staff should be vigilant to reduce the risks of virus infection as stated in the AUP.

The installation of software unauthorised by the school, whether licensed or not, is forbidden. If you are unsure, please speak to the head teacher and/or the Computing Subject leader for advice. The school reserves the right to examine or delete any files that are held on its system.

Some teaching staff are provided with a laptop computer for the purposes of planning, preparation and assessment and these should be used within this remit. The laptop computers remain the properly of the school and should be returned upon request. To use the internet at home, staff will need to change the internet settings as required. Antivirus, firewall and other management software must not be uninstalled.

**Network**

Staff will be issued with a username for the computer system and a simple password. It is their responsibility to change this in accordance with the password procedure below.

Pupils in Reception will not be expected to log on to the network and this may be done for them. From Year 1, children are expected to use their own individual logins for the system.

There are three categories of user on the system: pupils, admin and staff. Each level is managed by ONE ITSS who provide the support and infrastructure for our computer system.

**Backups**

Every school day the main server is set to backup essential files and settings. This is undertaken by ONE ITSS as part of their service level agreement.

**Security**

• All ICT equipment will be noted in the school inventory

• Any equipment taken off site should be signed out using the log book in the main office.

• The ICT Technician will be responsible for regularly updating anti-virus software

• Use of ICT will be strictly in line with the school’s ‘Acceptable Use Policy for Staff’

• Parents/carers will be made aware of the ‘Acceptable Use policy for Children’ and will be asked to counter-sign this with their child.

• All pupils and parents will be aware of the School Rules for Responsible Use of ICT and the Internet and will understand the consequence of any misuse.

The internet may be accessed by staff and by children throughout their hours in school. Filtering is provided as part of our service level agreement with ONE ITSS.

The teaching of email and internet should be covered within the Computing curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet.

All staff will be issued with a school email address and this is the email with which they should use for professional communication. Staff use the sbcschools.org.uk email system which is provided as part of our service level agreement with ONE ITTS. Further information about acceptable use can be found the acceptable use area of this policy.

Staff should take extra care to ensure that all communication with children and/or parents remains professional. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails and SeeSaw messages to ensure it is not misconstrued. All web activity is monitored by ONE ITSS so it is the user’s responsibility to ensure they log off appropriately. If children receive an email that they believe to be inappropriate then they should forward it on to their teacher and/or the E-Learning Leader who will investigate.

The use of the internet to access inappropriate materials such as auction sites, pornography, racist or any other material is prohibited. If users, especially children, do see an inappropriate website or image, they should close this immediately and report the site to the class teacher who should then report it to ONE ITSS and the E-Learning Leader.

**Passwords** (Linked to 360Safe Password Guidelines)

Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers. These should be changed regularly, especially if the user suspects others may know the password.

Children are provided with a username and password which we aim to make generic across the computer system and online services (with the exception of some sites requiring a prefix or a different username/password). Children should be taught not to share passwords and the reason for this. If a child suspects that their password has been compromised then they should tell their class teacher who should report it to the Computing Subject Leader who will then change the password.

**Age Limits**

Certain online tools have age limits on the use of their software. This is due to an Act of United States Law. The Children’s Online Privacy Protection Act prevents websites collecting data or providing their services to users under the age of 13.

As a school, we may decide to use some of these tools within lessons but will do so after thoroughly testing them for their safety and appropriateness. We will also post details of these sites on our school webpage. We will ensure that these will tend to be sites that allow creation of content rather than searching other users’ content.

Occasionally these sites will be used by teachers with a class, for example to create a class book or movie, but not by a child with their own personal account. We will make parents aware of this during our e-safety events. If they do not wish their child to access these sites, their child can be provided with an alternative method to complete the task.

**Health and Safety**

The school is aware of the Health and Safety issues involved in children’s use of digital technologies and follows the recommendations made by Stockton Borough Council. The school will dispose of redundant ICT equipment responsibly, safely and appropriately through ONE ITSS.

**Administrative Systems**

• The school administration will remain separate from the curriculum system. Class teachers have access to SIMs for registration with their own log in. Access to the rest of the system is only available to members of the Senior Leadership and Management Team and members of the school office.

• All staff members have a school email account through the sbcschools.org.uk email system

**Technical Support**

Most issues should be dealt with my ONE ITSS as part of our service level agreement. Issues can be logged on an online help desk, link found on staffs desktop which is provided by ONE ITS. Many minor issues are dealt with by the Computing Subject Leader.

**Social Media**

The school recognises that many staff will actively use Facebook, Twitter and other such social networking, blogging and messaging services. We also recognise that social media and networking sites are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks. Although these networks are used by staff in their own time, staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks. Staff are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.

Staff should:

* Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
* Not accept current or ex-pupils as ‘friends’ who are still minors on social media sites such as Facebook, Instagram, Snapchap, OoVoo etc. This is to ensure any possible misinterpretation. It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors. We do understand that some staff members have friends within the local community (such as children’s parents) and ask that these members of staff take extra precaution when posting online.
* Ensure that if their communication is fully public (e.g. blogs/Twitter), or is visible to parents of children within the school community, that they maintain their professionalism at all times and remember that they are a representative of the school even out of school hours and at weekends.
* Be aware that electronic texts can sometimes be misinterpreted or misconstrued so should endeavour to minimise the possibility of this happening.

Instances of online behaviour, including those on social media and the internet, which could be perceived to have a negative or detrimental impact or effect upon the reputation of the school will not be tolerated or supported by the governing body. Staff should report any instances of unacceptable online behaviour to the Head Teacher and/or Chair of Governors who will follow the staff code of conduct/school’s disciplinary procedure.

Pupils should not be signed up to most social networking sites due to the over-13 age limit.

**E Safety**

Children should also be encouraged to discuss their online activities with parents and teachers in an open and honest way, knowing who to approach if they have any concerns.

* Parents and carers must play an active role in the monitoring of their children’s E-safety and will be encouraged to engage in an open dialogue with school. High Clarence Primary School will take steps to provide up to date E-safety guidance from recognised organisations such as the Child Exploitation, Online Protection Centre (CEOP) and Childnet International. A record of this will be kept in the office with any bullying incidents.

**Managing Website Content**

* Editorial guidance will ensure that the school’s ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
* Parents must sign the school parental consent form for photographs of pupils to be used. If a child does not have consent then the school is responsible for ensuring that no photographs of the child are used.
* The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupil’s home information will not be published.
* The headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.
* The website will comply with the school’s guidelines for publications
* Use of site photographs will be carefully selected so that any pupils cannot be identified or their image misused.
* The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.
* Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

**Digital and Video Images**

At High Clarence Primary School uses children’s photographs to add colour, life and interest to promote school activities and initiatives. They can increase pupil motivation and staff morale, and help parents and the local community identify and celebrate the school’s achievements. However, photographs must be used in a responsible way. Schools need to respect children’s and parents’ rights of privacy and be aware of potential child protection issues.

At High Clarence Primary School every reasonable effort will be made to minimise risk by following the guidelines detailed in this Public Image Policy and by securing parental consent for the use of photographs.

This policy applies to the use of photographs on the school network, on its VLE and in the press.

This policy reflects the consensus of opinion of the staff and governing body of High Clarence Primary School. Its implementation is the responsibility of all staff. Parents and visitors will be made aware of this policy.

**Child Protection**

There may be a risk when individual pupils can be identified in photographs. For that reason the governing body of High Clarence Primary School have developed this policy to make every effort to minimise risk.

In the event of the inappropriate use of children’s photographs the Headteacher will inform the local Child Protection Officer and Social Services and/or the Police.

# **Data protection**

High Clarence Primary school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation (GDPR)](http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/18153.pdf).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Photographs and video images of pupils and staff are classed as personal data under the terms of the DPA 2018, therefore, using such images for school publicity purposes requires the consent of either the individual concerned or in the case of pupils, their legal guardians.

**Appropriate Use of Pupil Images**

The staff and governors of High Clarence Primary School will:

* Ensure that electronic images are stored on a secure network to which members of the public have no access;
* Secure parental consent for the use of children’s photographs;
* Only photograph children in swimming costume from the waist up.
* Newspapers tend to want to put the names of pupils in photographs. Further parental consent will be gained and it is made clear that the photograph will be published in a newspaper.
* Images will be used in children’s work as part of planned lessons, some examples of how images will be used are to celebrate school’s successes, recounts of school visits
* Photos of children and their work will be uploaded and stored on SeeSaw so parents can view it. SeeSaw is password protected which all users have their own unique usernames and password.

**Filming School Events**

Parents and spectators may want to photograph or video an event at school, such as a sports day or an arts performance. This does not cause school any problems as long as parents are fully aware of our expectations. The process is as follows:-

* Headteacher asks at the beginning of concerts, special assemblies, events if parents agree to the event being photographed or filmed
* Common practice will be that permission will be given to parents and relatives known to the school and that there is an implicit understanding that any image created will be solely for the use of parent or relative taking the image.
* Any parent who has a concern regarding the taking of images at an event should contact the Headteacher immediately.

## E Safety

## High Clarence Primary we take E-safety very seriously. We will ensure that it is taught often throughout the children’s Computing and Personal Development curriculum. We will also provide children with dedicated e-safety lessons where appropriate. Children will be taught how to act online and how to minimise the risk when working on the internet. Pupils will also be taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them.

## All children will be taught about the Acceptable Use Policy and will sign a copy related to their age phase. These will be stored by the Admin Team. All staff will also complete an AUP.

## If a teacher suspects an E-safety issue within school they should make notes related to the incident in accordance to anti-bullying and behaviour policies. This should then be reported to the head teacher and recorded as appropriate.

## If children receive an email that they believe to be inappropriate then they should show it to their teacher and/or the head teacher who will investigate.

**Monitoring & Breaches**

The Computing Subject Leader or member of the SLT may inspect any ICT equipment owned or leased by the school at any time without prior notice.

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

**Incident**

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school’s relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: The Computing Subject leader or member of the SLT.

All e-safety incidents should be logged on the school’s CPOMS service.

**Dealing with complaints**

* Staff, children and young people, parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the school’s Safeguarding Policy and Procedures.
* The school’s designated person for e-safety, N Caraher who will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the headteacher immediately.
* Pupils and parents/carers will be informed of the complaints procedures.
* Parents/carers and pupils will work in partnership with the school staff to resolve any issues.
* As with drugs issues, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence. Parents will also be informed.
* Sanctions for misuse may include any or all of the following:
* Interview/counselling by an appropriate member of staff
* Informing parents/carers
* Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system
* Referral to the police if it is felt necessary

**Inappropriate Material**

* All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher.
* Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
* Users are made aware of sanctions relating to the misuse or misconduct through the acceptable use policy.

**Mobile Phones**

Pupils are not permitted to bring mobile phones to school. On an occasion when this accidentally happens they will be handed in at the school office, where they will be locked away until the end of the school day.

* As a general rule, staff should not make or receive calls, or send texts or access social media except at lunchtimes or during break.
* Mobile phones turned off or to be on silent while the employee is at work.
* If there is a specific reason to keep mobile on for a limited time, staff may request permission from SLT.
* Phone generally stored away from view.
* A school device should be the preferred option to take photos and videos of students. If staff use the camera on their mobile phone to take photos or videos of the students then they should be saved onto school devices and deleted from personal devices.
* Employees are encouraged not to use their phones in classrooms, playground, or any other area where pupils are present unless it’s to enhance lessons.

**Introducing the Policy to pupils**

* Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet.
* Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

**Parents/Carers Support**

* Parents/carers will be informed of the school’s Internet Policy which may be accessed on the school website, in the school brochure and by forms which they sign when their child starts school.
* Any issues concerning the internet will be handled sensitively to inform parents/carers without undue alarm.
* A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.

**Community Use**

* School Computing resources may be increasingly used as part of the extended school agenda.
* Adult users will sign the school’s Acceptable Use Policy.

Appendix 1 – Acceptable Internet Use Staff Policy

Appendix 2 – Acceptable Email Use Staff Policy

Appendix 3 – Acceptable Internet and Email Use Pupils Policy

Appendix 4 – Pupil Images

Appendix 5 – Social Networking Policy

Appendix 6 – Laptop Protocol for Teachers and School Support Staff

#### Appendix 1

**ACCEPTABLE INTERNET USE POLICY FOR ALL SCHOOL STAFF**

**The Importance of the Internet in Learning**

The purpose of Internet access in school is to raise educational standards, to support professional work of staff and to enhance the school’s management information and business administration systems. Access to the Internet is a necessary tool for staff and pupils. It is an entitlement for pupils who show a responsible and mature approach.

**Using the Internet to provide effective learning.**

Teachers, parents and pupils need to develop good practice in using the Internet as a tool for teaching, learning and communicating. There is a fine balance between encouraging autonomous learning and maintaining adequate supervision. Systems that ensure internet use is as safe as possible will enable increased use and quality. Internet access is provided by the LA. This includes a filtering system (cache pilot).

* Internet access will be planned to enrich and extend learning activities.
* Access levels will be reviewed to reflect the curriculum requirement.
* Pupils will be given clear objectives for Internet use.
* Staff will select sites that will support the learning outcomes planned for pupils’ age and maturity.
* Pupils will be educated in taking responsibility for Internet access.

The computer network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. This policy was drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer network and to monitor any Internet sites visited.

* I will only use the school’s Internet and any related technologies for professional/educational purposes or for uses deemed ‘reasonable’ by the Headteacher or Governing Body.
* I will ensure that the children using the Internet in school are supervised at all times.
* I will comply with the Computing network security policy statements and not disclose to anyone any passwords provided to me by the school or other related authorities.
* I will ensure that children’s personal data (such as data held on SIMS) is kept secure and used appropriately, whether in school, taken off the premises or accessed remotely.
* I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Headteacher.
* I will respect copyright and intellectual property rights; this includes downloadable and other materials.
* I will not deliberately seek out inappropriate/offensive materials on the Internet and I am aware I will be subject to the LA’s recommended disciplinary procedures should I do so.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Computing Subject Leader.

Full name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ post \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Approved \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Appendix 2

**ACCEPTABLE EMAIL USE POLICY FOR ALL STAFF**

E-mail is an essential means of communication within education. Staff will be given a “professional” e-mail account. The staff are at liberty to use their accounts for correspondence between one another or other professional bodies as part of their work. The Administrator has the right to reset passwords where there is good reason to do so.

Staff will also be expected to report any offensive e-mails that they receive to the Headteacher. Any intercepted e-mails or reports of offensive e-mails will be reported to the Headteacher.

Failure to adhere to the agreement will result in suspension of the use of the internet and e-mail accounts, pending a resolution.

* Staff must use the school e-mail address if they need to communicate with pupils about their school work
* Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail
* Access in school to external personal e-mail accounts may be blocked
* The forwarding of chain letters or similar is not permitted
* Incoming e-mail should be monitored and attachments should not be opened unless the author is known

Staff should sign a copy of this Acceptable Email Use Policy and return it to the Computing Subject Leader.

Full name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ post \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Approved \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 3**

Dear Parents,

**ACCEPTABLE INTERNET AND EMAIL USE POLICY FOR PUPILS**

As part of pupils’ curriculum enhancement and the development of Computing skills, High Clarence Primary School is providing supervised access to the Internet including e-mail. Although there are concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school.

The internet we receive into school is provided by Northern Grid using a company called Easynet. This operates a filtering system and restricts access to inappropriate materials. To help you in this respect at home, we have included a weblink with sources of information about Safe Internet Access.

<http://www.staysafeonline.info/>

<http://www.ceop.gov.uk/>

<http://www.thinkyouknow.co.uk/>

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, Stockton Borough Council cannot be held responsible for the nature or content of materials accessed through the Internet. The Council will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities.

We enclose a copy of the Rules for Responsible Internet and Email Use that we operate at High Clarence Primary School. Please spend a time with your child discussing these rules making sure that they understand them. Should you wish to discuss any aspect of Internet use please don’t hesitate to get in contact.

Yours sincerely

N Caraher

Headteacher

**Rules for Responsible Internet and Email Use**

* I will use only my own login and password, which I will keep a secret.
* I will not access other people’s files.
* I will use the computers only for schoolwork and homework.
* I will not bring USB (storage devices) into school without permission.
* I need permission from a member of staff before using the internet.
* I will only e-mail and open up e-mail attachments from people I know, or my teacher has approved.
* I will not deliberately look for, save or send anything that could be unpleasant or nasty.
* I will not give my home address or phone number, or arrange to meet someone, unless my parent or teacher has given permission.
* I will tell an adult if I see anything I am unhappy with or I receive a message I do not like.
* I understand that school can check my computer files, e-mail account and the Internet sites I visit.
* I will be responsible for my behaviour when using Computing because I know that the rules are to keep me safe.

**Parent Agreement:**

I have read and discussed the Rules for Responsible Internet and Email Use with my child.

**Signed:**

**Print Name:**

**Date:**

**Pupil Agreement:**

I agree to follow the Rules for Responsible Internet and Email Use**.**

**Signed:**

**Print Name:**

**Date:**

**Appendix 4**

Dear Parents,

**Public Images**

High Clarence Primary School takes photographs of children to celebrate successes and educational purposes. We may wish to use a photograph of your child for our brochure or website in the future. Additionally, photographs are published in newspapers. If a photograph of your child is used in a publication, we will not disclose the name without asking your permission.

To comply with the Data Protection Act 1998, we need your permission before we use any photograph that we have taken.

Please complete the declaration below and return it to us.

I give permission for my child’s photograph to be taken and used by High Clarence Primary School.  
I have read and understood the conditions of use

Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of Child \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 5**

**SOCIAL NETWORKING POLICY FOR STAFF IN SCHOOLS**

Introduction

The Governing Body of High Clarence Primary School is committed to ensuring that all staff are aware of their responsibilities in connection with the growing use of social networking sites. It recognises that the use of such sites have become a very significant part of life for many people. They provide a positive way to keep in touch with friends and colleagues, and can be used to exchange ideas and thoughts on common interests. Examples of such sites include, but are not limited to, blogs (short for web log), MySpace, Facebook, Bebo, YouTube, Windows Live Spaces, MSN, forums, bulletin boards, multiplayer online gaming, chatrooms and instant messenger.

Staff are expected to keep a professional distance from pupils and there should be a clear separation of the private social lives of staff and that of pupils.

It is important that staff are able to use technologies and services effectively and flexibly whilst ensuring that they do not make themselves vulnerable. However, it is also important to ensure that this is balanced with the Governing Body’s duty to safeguard children, the reputation of the school, the wider community and the Local Authority.

Who does this policy apply to?

This policy will apply to all staff in schools whose contracts of employment have been issued by the Local Authority on behalf of the Governing Body, including Community and VA Schools.

Aims

The policy aims to:

* Enable employees to use social networking sites safely and securely;
* Ensure that employees are aware of the risks associated with the inappropriate use of social networking sites;
* Safeguard employees in connection with the use of social networking sites and ensure they do not make themselves vulnerable;
* Ensure the Governing Body maintains its duty to safeguard children, the reputation of the school, the wider community and the Local Authority.

Legislation

The following legislation must be considered when adhering to this policy:

* Human Rights Act 1998
* Data Protection Act 1998
* Freedom of Information Act 2000
* Computer Misuse Act 1990, amended by the Police and Justice Act 2006

Responsibilities

The Governing Body (in conjunction with the Local Authority) shall:

* Ensure this policy is implemented and procedures are in place that deal with the use of social networking sites;
* Ensure that all employees have access to this policy and that new employees are made aware of it.

Headteachers/SLT:

* Be familiar with this policy and guidelines and ensure that employees understand the policy and their own responsibilities;
* Ensure that staff are aware of the risks of the use of social networking sites and the possible implications of the inappropriate use of them;
* Instigate disciplinary procedures where appropriate to do so;
* Seek advice where necessary from Human Resources on the approach to be adopted if they are made aware of any potential issue.

Staff shall:

* Behave responsibly and professionally at all times in connection with the use of social networking sites;
* Co-operate with management in ensuring the implementation of this policy.

Human Resources shall:

* Provide the necessary professional advice and support to the Governing Body and all school staff when required.

Use of Social Networking Sites

For employees’ own security all communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. It is therefore advised that staff follow the following procedures:

* Staff must not access social networking sites for personal use via school information systems or using school equipment;
* Staff must not accept pupils as friends – personal communication could be considered inappropriate and unprofessional and makes staff vulnerable to allegations;
* Staff are advised not to be friends with recent pupils. The potential for staff to be compromised in terms of wall content and open to accusations makes the risk not worth taking;
* Staff should not place inappropriate photographs on any social network space;
* Staff should not post indecent remarks;
* If a member of staff receives messages on his/her social networking profile that they think could be from a pupil they must report it to their Line Manager/Headteacher and discuss whether it is appropriate to contact the internet service or social networking provider so that they can investigate and take the appropriate action;
* Staff are advised not to write about their work but where a member of staff chooses to do so, he/she should make it clear that the views expressed are his/hers only and do not reflect the views of the school/Local Authority. However, all other guidelines in this policy must be adhered to when making any reference to the workplace;
* Staff must not disclose any information that is confidential to the school or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act;
* Staff must not disclose any information about the school/Local Authority that is not yet in the public arena;
* In no circumstances should staff post photographs of pupils;
* Staff should not make defamatory remarks about the school/colleagues/pupils or the Local Authority or post anything that could potentially bring the school/Local Authority into disrepute;
* Staff should not disclose confidential information relating to his/her employment at the school;
* Care should be taken to avoid using language which could be deemed as offensive to others.

Breaches of the Policy

The Governing Body does not discourage staff from using social networking sites. However, all staff should be aware that the Governing Body will take seriously any occasions where the services are used inappropriately. If occasions arise of what could be deemed to be online bullying or harassment, these will be dealt with in the same way as other such instances.

If any instances of the inappropriate use of social networking sites are brought to the attention of the Headteacher, depending on the seriousness of the allegations, disciplinary action may be taken.

There may be instances where the School or Local Authority will be obliged to inform the police of any activity or behaviour for which there are concerns as to its legality.

Staff should sign a copy of this **Social Networking Policy for Staff in school** and return it to the Computing Subject Leader.

Full name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ post \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 6**

**High Clarence Primary School**

**LAPTOP PROTOCOL FOR TEACHERS AND SCHOOL SUPPORT STAFF**

This protocol is designed to act as a guide and simple framework upon which the use of laptops by teachers or school support staff should be based. The intended spirit of the list is to act as a reminder on use and security.

* The ownership of the laptops rests with the school.
* Teachers/support staff have full use of the laptops to develop planning, curriculum subject and Computing experience.
* Teachers/support staff are free to install software appropriate to their professional needs on the laptops providing all licences are kept securely.
* No restrictions or barriers are placed on Internet access; staff are free to choose their own ISP and are responsible for any charges incurred.
* Teachers/support staff are reminded that they should not deliberately seek out inappropriate/offensive materials on the internet and that they are subject to the LA’s recommended disciplinary procedures for teaching and non-teaching staff should they do so.
* Anti-virus software is provided with each laptop and members of staff have the responsibility of keeping the software up-to-date and for scanning materials downloaded from the Internet.
* Teachers/support staff should always password protect important or sensitive information, and ensure that back-up copies of such information are taken and held securely.
* There are a number of legal requirements relating to the use of information and software (e.g. Data Protection Act, Copyright Act). Teachers/support staff are responsible for understanding and complying with their legal requirements. Advice and guidance is available from the Stockton Schools Extranet.
* Teachers/support staff should be aware that laptop computers have a high re-sale value and that they should never be left in cars or in a place where an opportunist could take it. With most insurance companies laptops are covered in cars as long as they are not left unattended.
* Teachers/support staff should make sure that they are aware of the arrangements that have been made by the school for insurance cover on laptop computers and to follow any guidelines/procedures established by the school to safeguard this cover.
* Be aware of the school’s policy on the use of laptops and the school network.

Staff should sign a copy of this Laptop Protocol and return it to the Headteacher.

Full name ……………………………… post ………………………………

Signed ……………………………… date ………………………………

Approved ……………………………… date ………………………………