Bowesfield Primary School

eSafety Policy

Guidance for the acceptable use of ICT

Our Vision for ICT

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Schools need to build in the use of these technologies in order to equip young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Bowesfield Primary School we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Our school holds personal data on learners, staff and other people to help us conduct our day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our school to use technology to benefit learners.

Everybody in our school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Equal Opportunities

Pupils with Additional Needs

Our school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Michelle Jobling who works closely with the Headteacher and senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Stockton LA, OFSTED, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in ICT/ PSHE lessons which will be tracked through planning and progression statements (***ICT scheme of work, PSHE medium term planning***.)

- The school provides opportunities within a range of curriculum areas to teach about eSafety

- Educating pupils on the potential risk of inappropriate use of technologies that maybe encountered outside school is done informally when opportunities arise.

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities

- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

- Pupils are taught to be discerning users of ICT and critically evaluate materials found online and learn effective searching skills

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety issues to ensure they are up to date with the latest guidance
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)
- All staff will incorporate eSafety activities and awareness within their curriculum activities

Managing the School eSafety Messages

- ESafety messages are embedded across the curriculum whenever the internet and/or related technologies are used
- The eSafety policy is reinforced to the pupils at the start of each school year
- eSafety posters are prominently displayed around school

Managing Other Web 2 Technologies

We believe that Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative facilities. However it is important to recognise that there can be issues regarding the appropriateness of some content and contact. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils and their parents/carers are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- Our pupils are asked to report any incidents of bullying to the school
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Headteacher

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We strive to work in partnership with parents/ carers and to discuss eSafety and seek to promote a wide understanding of the benefits related to ICT and potential risks.

- Parents/ carers and pupils are actively encouraged to contribute to reviews of the school eSafety policy
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to eSafety where appropriate in a variety of forms

Acceptable Use Policies

As a school we have produced a number of policy statements which we deem to be acceptable use of a range of technologies in school.

Appendix 1 - *Acceptable Use Policy: Pupils*

Appendix 2 - *Acceptable Use Policy: Letter to parents*

Appendix 3 - *Digital Images Policy*

Appendix 4 - *Digital Images Policy: Parent Permission Slip*

Appendix 5 - *Staff ICT Acceptable Use Policy 2012*

Appendix 6 - *Staff Social Networking Policy*

Appendix 7 - *Mobile Phones in School Policy*

Appendix 8 - *Acceptable Use Policy: Visitors*

Appendix 9 – *Additional Guidance for staff*

Monitoring

Authorised staff may inspect any ICT equipment owned or leased by the School at any time without prior notice.

Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Breaches

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

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedures.

Policy breaches may also lead to criminal or civil proceedings.

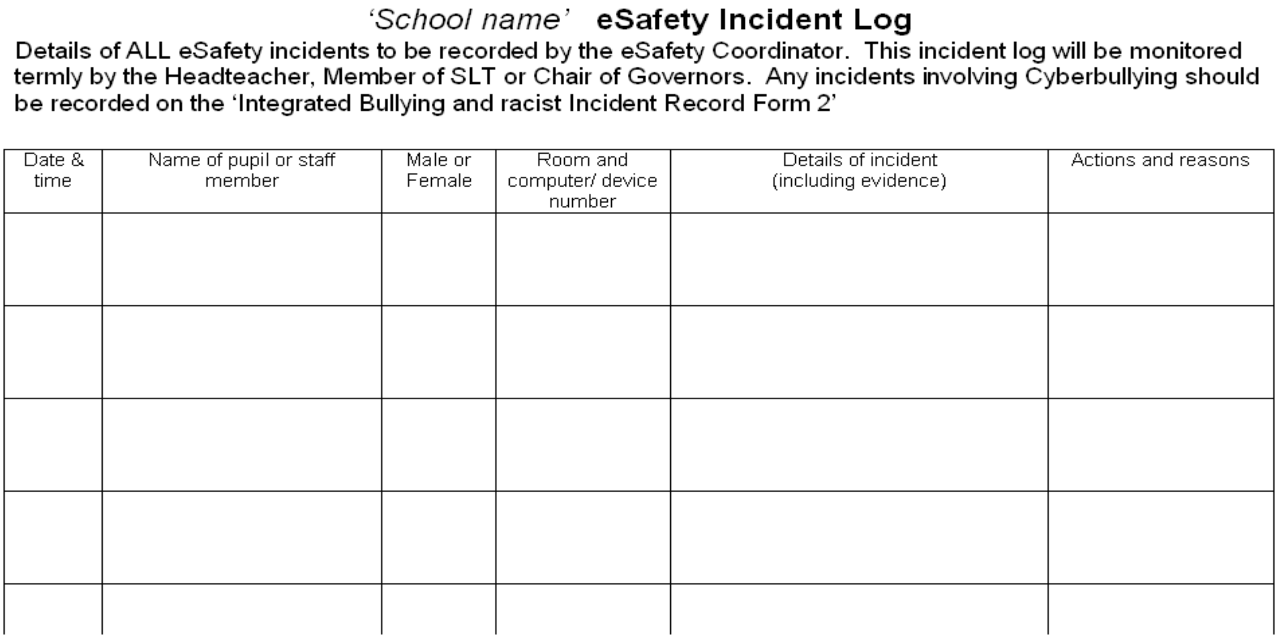
Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to Miss Hodgeon or Miss Jobling. 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 Miss Hodgeon or Miss Jobling.

Incident Reporting, Log & Infringements

eSafety Incident Log

Some incidents may need to be recorded in other places in line with the schools anti bullying policy.



'School name' **eSafety Incident Log**

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher and incidents should be logged. Where appropriate the complaints policy and procedures will be consistently followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct

Writing and Reviewing this Policy

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them

There will be an on-going opportunity for staff, pupils, parents and carers to discuss any issue of data security that concerns them

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning

The policy will be amended as new technologies are adopted

This policy has been read and approved by the staff, head teacher and governors

Appendices

Appendix 1 - Acceptable Use Policy: Pupils

Primary Pupil Acceptable Use Agreement

- I will only use ICT in school for school purposes.
- I will only e-mail people that my teacher has approved.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone I have met online unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive a message I do not like.
- I will not bring removable media into school without permission.

Appendix 2 - Acceptable Use Policy: Letter to parents

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc has become an important part of learning in our school.   We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Miss Hodgeon or Miss Jobling,

- - ✂- · -

Parent/ carer signature
We have discussed this and ………………………………………..........(child name) agrees to follow the Acceptable use agreement and to support the safe use of ICT at Bowesfield Primary School.

Parent/ Carer Signature …….…………………..………………………….

Appendix 3 - Digital Images Policy

Working with children and young people may involve the taking and recording of images – to record events in school or collect evidence of work for assessment.

Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people.

At Bowesfield, parents or carers are asked to sign to confirm that they are aware that images may be taken, and give their permission for this to happen, as their child is admitted to school. Children are informed of the reason for the photo being taken.
The member of staff taking the photo needs to check photo permission prior to any photos being taken. *Some parents / carers may agree to have their child's photo taken and used in displays in school, but not published anywhere other than in school, and not uploaded to the website. This must be discussed by individual staff with parents / carers and the discussion recorded on the permission booklet, initialled and dated by staff and parent / carer.*

Information on the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the internet is included on the photo permission form.

All images must be taken only with school equipment and transferred within 1 school day to a file in staff shared / photographs, or deleted. As they are saved they must be deleted from the equipment. This is a secure area and only school staff have access to it. Photos will be saved until the children leave at the end of Y6 and then deleted.

Adults need to remain sensitive to any children who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings. If children appear uncomfortable for any reason, please allow them to choose not to be part of the photo.

It is not appropriate for adults to take photographs of children for their personal use.

All adults must ensure they:

- *are clear about the purpose of the activity and about what will happen to the images when the activity is concluded*

- *are able to justify images of children in their possession and able to explain when they will transfer them to staff shared*

- *avoid making images in one to one situations or which show a single child with no surrounding context*

Appendix 4 - Digital Images Policy: Parent Permission Slip

The following text is taken from the Permission to take and use photos and digital images

Photos of children are often used to record school events, or to use for assessment, and may be displayed and shared in the following ways.

In the entrance of school, on the screen, for visitors and people in school to see
On display boards around school
On the school website
On the websites of places that the children visit
In the media, including online publications

We assure you that all staff have agreed that:

We will only take, and use photos as part of assessments, or when recording school events.

We will always consider the privacy, dignity, safety and well-being of your child.

We will only use school cameras, or other authorised equipment for photos of children.

Photos will be promptly downloaded to a secure computer file, which only staff have access to. They will then be deleted from cameras.

Photos will be permanently deleted from the file when your child leaves at the end of Y6.

We will not identify your child by name when displaying photos.

Any staff new to school will be asked to sign to say that they agree with this policy.

Visitors are asked not to have their mobiles / cameras in areas where there are children.

If any other professionals ask to take photos as part of their work, they will have to follow the same guidance as school staff.

For safeguarding reasons we need to have parental consent to take and use photos of children. Please sign the permission slip to give your consent for photos of your child to be taken and used, within the guidelines above, while they are at Bowesfield.

If you have any concerns at all, at any time, please come and ask.

Name of child:

Date:

I give permission for photos of my child to be taken and used, within the guidance provided, while they attend Bowesfield Primary School.

I understand that I have the right to change my mind and withdraw this permission at any time but that I must inform the school in writing of this.

Signed: Parent / Carer

Thank you for your support in keeping your child safe.

Appendix 5 - Staff ICT Acceptable Use Policy 2012

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school digital image use policy and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the School Learning Platform to upload any work documents and files – into a secure area, ensuring that only relevant people can access them. I will protect the devices in my care from unapproved access or theft by not leaving them vulnerable e.g. in an unattended car.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.

- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces

- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Officer (Emily Hodgeon) and/or the e-Safety Coordinator (Michelle Jobling) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Michelle Jobling) the e-Safety Coordinator or (Stockton ICT Unit) the designated lead for filtering as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the SICTU as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Stockton Borough Council, into disrepute.

- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator (Michelle Jobling) or the Head Teacher.

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of ~~I~~information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ……………………….... Print Name: …………………… Date: ………

Accepted by: ………………………….. Print Name: ………………………..

Appendix 6 - Staff Social Networking Policy

The following text has been adopted from the Stockton Borough Council Social Networking Policy for Staff in SChools

1.0 Introduction
The Governing Body of …………..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. There is no need for social networking to go on between staff and pupils and there is no clear educational benefit.

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.

2.0 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. It does not apply to supply staff employed by agencies.

3.0 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.

4.0 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

5.0 Responsibilities
5.1 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.

5.2 Headteachers/Line Managers shall:

- 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.

5.3 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.

5.4 Human Resources shall:

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

6.0 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.

7.0 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.

Appendix 7- Mobile Phones in School Policy

Staff and visitors to school often carry a mobile phone, either for personal or work use.

Having mobile phones in use while children are present could potentially place children at risk, and leave staff / visitors open to allegations.

Potential risks are:

- phones being used to take images of children
- staff / visitors having images of children stored on their personal phones
- children overhearing private / personal / confidential conversations
- phone calls interrupting learning
- unauthorised access to inappropriate internet sites
- unauthorised access to personal data, including images

The phones of staff members, students and volunteers must be switched off and stored either in a locker, or a locked cupboard within the classroom / office, with the key stored securely.

From the time children start to come into school for breakfast club; staff, students and volunteers must only use their phones in the administrative area of school (staffroom or office) during breaks or lunchtimes, where no children are present. Once all children have left for the day (including those attending clubs), staff not involved in meetings may use phones in any area, but need to be aware that other adults may overhear their calls.

The school phone number (01642 601890) can be given by staff as an emergency contact. If callers ask for a member of staff who is teaching, they will be asked if it is urgent – and in any emergency, the member of staff will be called to the phone.

All visitors to school, including parents / carers attending workshops, meetings or assemblies, will be asked to switch off their phones and hand them in at the office, to be stored securely, until their departure. A record of phones handed in is kept and visitors need to sign to say they have been given their phone back as they leave. Parents visiting the office / Headteacher for drop in discussions are accompanied by a member of staff at all times and do not need to hand their phones in.

Children may not have mobiles in school and any phones brought in by children will be stored securely in the office until collected by a parent / carer.

Staff accompanying children on out of school must use school mobiles (pre-loaded with the school number, HT's office number and the numbers of the school mobiles) so that they can make contact with school / each other in an emergency. These mobiles do not include cameras, recording equipment or internet access.

Any concerns or questions regarding mobile phones in school, including unauthorised or inappropriate use, must be raised with the Headteacher, or, if the Headteacher is unavailable, the Deputy Headteacher.

Appendix 8 - Acceptable Use Policy: Visitors

Visitors
Acceptable Use Agreement

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all visitors are aware of their professional responsibilities when using any form of ICT. All visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Miss Jobling or Miss Hodgeon.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will not install any hardware of software without permission of Miss Hodgeon or Miss Jobling
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- 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 Headteacher.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will ensure that through my online activity, in school, I will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school
Signature …….………………………… Date ……………………

Full Name ……………………………………………………………..(printed)

Job title . . . .

Organisation ……………………………………………………

Appendix 9 - Additional Guidance for Staff

e-Mail:

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- Staff must inform (Miss Hodgeon or Miss Jobling) if they receive an offensive e-mail

- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information

- Use your own school e-mail account so that you are clearly identified as the originator of a message

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail

- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly
- Activate your ‘out-of-office’ notification when away for extended periods
- Use the ‘Delegation’ facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)
- Never open attachments from an untrusted source; Consult your network manager first.

e-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted
- Where your conclusion is that e-mail must be used to transmit such data:
  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

Internet Access

Managing the Internet

- Staff will preview any recommended sites before use
- Image searches are discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog

It is at the Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastucture

- School internet access is controlled through the LA's gate keeper filtering service. For further information relating to filtering please go to a member of staff in school or contact the Stockton ICT Unit personally
- Our school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff are aware that internet activity can be monitored and explored further if required
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines
- Staff using removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems.

If there are any issues related to viruses or anti-virus software, ICT subject leader should be informed

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to connect their ICT hardware to the school network points (unless provision has been made).
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- A time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles
- On termination of employment, resignation or transfer, return all ICT equipment. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

- All activities carried out on School systems and hardware will be monitored
- Staff must ensure that all school data is stored on school's network, and not kept solely on a mobile device. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Strong passwords are encouraged
- User ID and passwords for staff and pupils who have left the School are removed
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)

If you think your password may have been compromised or someone else has become aware of your password report this to Miss Hodgeon or Miss Jobling

Computer Viruses

- Never interfere with any anti-virus software installed on school ICT equipment that you use
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know