Bexton Primary School

Together we can make a difference

e-Safety Policy

Name of school: **Bexton Primary School**

Date of review: **Summer 2013**

New review date: **Summer Term 2014**

Background / Rationale

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

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has the potential to raise educational standards and promote pupil achievement.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

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

and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

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

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents & visitors) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour that take place out of school.
Bexton Primary School is proactive in the education of pupils in regard to establishing what bullying is and providing advice and guidance to parents, encouraging them to take responsibility for their children's online activities.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports where necessary. A member of the Governing Body has taken on the role of e-Safety Governor.

The role of the E-Safety Governor will include:
- regular meetings with the E-Safety Co-ordinator / Officer
- regular monitoring of e-safety incident logs should they occur
- reporting to relevant Governors committee

Headteacher and Senior Leadership Team:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator

- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher and Child Protection officer should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

In the case of an allegation against the Head or the Child Protection officer, another member of the Senior Leadership Team will be asked to follow procedures. Please see policy on Allegations of abuse against staff for further guidance.

E-Safety Coordinator :

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents, should they occur, to inform future e-safety developments
- meets regularly with the E-Safety Governor to discuss current issues
- attends relevant committee meetings of Governors

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator / Headteacher / Senior Leader / ICT Co-ordinator / Class teacher for investigation
- digital communications with students / pupils (email / blogging / messaging / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and how to stay safe on the internet
- they monitor ICT activity in lessons, extracurricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Staff have a professional responsibility for ensuring that they meet the guidelines of the School Acceptable Use of ICT Policy (which includes the use of mobile phones, cameras and other hand held devices) and ensuring that their activities outside of school do not bring the reputation of the school or individuals within the school into disrepute.

Designated person for child protection / Child Protection Officer

should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming

- cyber-bullying

Students / pupils:

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying (in particular KS2).
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings / information sessions, newsletters, letters, website and information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:

- endorsing the Student / Pupil Acceptable Use Policy
- accessing the school website / Blog in accordance with the relevant school Acceptable Use Policy.

Policy Statements

New technologies have become integral to the lives of children at our school and young people in

Education – students / pupils

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

E-Safety education will be provided in the following ways:

- E-safety should be provided as part of ICT / PHSE and other relevant lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, and website
- Parents evenings / parent information sessions
- Reference to the CEOP / childnet / Kidsmart internet safety materials

Education & Training – Staff

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

- A planned programme of e-safety training will be made available to staff through formal INSET and staff meetings.
- All new and existing staff should sign to agree they fully understand the school e-safety policy and Acceptable Use Policies

Technical – infrastructure / equipment, filtering and monitoring

The school and Cheshire Shared Services ICT Department will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Bexton Primary School Security Policy and Acceptable Usage Policy and E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.

- All users will be provided with a username and password users will be required to change their password termly.
- The "master / administrator" passwords for the school ICT system, used by Cheshire Shared Services ICT Department must also be available to the School Business Manager.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by Cheshire East Local Authority.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to Cheshire Shared Services ICT Department.
- Requests from staff for sites to be removed from the filtered list will be considered by the School Business Manager and Head Teacher If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- Cheshire East Shared Services ICT Department regularly monitor and record the activity of users on the Cheshire ICT systems and users are made aware of this in the Acceptable Use Policy
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Head Teacher / Designated Safeguarding Person / School Business Manager.
- Appropriate security measures are in place) to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Any guests are able to access school computers using the "Guest" log on which provides limited accessibility to systems.
- All staff should adhere to the Acceptable Use of ICT Agreement which they should sign on an annual basis and relates to the extent of personal use that users are allowed on laptops and other portable devices that may be used out of school.
- Teachers may install "Apps" on iPads for the purposes of extending the school curriculum; these should be agreed as "fit for purpose" with the Head Teacher.
- The Acceptable Use of ICT Agreement outlines the policy surrounding the use of removable media by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured, encrypted sticks can be ordered from the school office.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use
- Where pupils are allowed to freely search the internet, eg using search engines, they are actively taught safe practice on internet search engines before use.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. Photographs should not be stored on remotely accessed sites e.g. Dropbox.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published in the local press or online (subject to school agreement)

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

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

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

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

Communications

.

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- Staff and pupils should only use the school email service to communicate on behalf of the school.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, pupils or parents (email, blogs etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**				√	√
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation				√	√
	adult material that potentially breaches the Obscene Publications Act in the UK				√	√
	criminally racist material in UK				√	√
	pornography				√	
	promotion of any kind of discrimination				√	
	promotion of racial or religious hatred				√	
	threatening behaviour, including promotion of physical violence or mental harm				√	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				√	
Using school systems to run a private business					√	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					√	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					√	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					√	
Creating or propagating computer viruses or other harmful files					√	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					√	
On-line gaming (educational)			√			
On-line gaming (non educational)					√	
On-line gambling					√	
On-line shopping / commerce for school purchasing				√		
File sharing					√	
Use of social networking sites					√	
Use of video broadcasting eg Youtube			√			

Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:
If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils Actions / Sanctions

Incidents: *Please note: After discussion with staff, it was agreed that the actions / sanctions would have to be dependent on severity / persistence of the incidents.*	Refer to class teacher / tutor	Refer to e-safety coordinator / SLT member	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	√	√	√	√	√	√	√	√	√
Unauthorised use of non-educational sites during lessons (dependent on severity)	√	√						√	
Unauthorised use of mobile phone / digital camera / other handheld device (dependent on severity)	√	√	√					√	
Unauthorised use of social networking / instant messaging / personal email	√	√	√			√		√	√
Unauthorised downloading or uploading of files	√	√	√			√	√	√	√
Allowing others to access school network by sharing username and passwords	√	√	√			√	√	√	√
Attempting to access or accessing the school network, using another pupil's account.	√	√	√			√	√	√	√
Attempting to access or accessing the school network, using the account of a member of staff	√	√	√			√	√	√	√
Corrupting or destroying the data of other users	√	√	√			√	√	√	√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature.	√	√	√	√		√	√	√	√
Continued infringements of the above, following previous warnings or sanctions	√	√	√	√	√	√	√	√	√

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√	√		√	√	√	√	√
Using proxy sites or other means to subvert the school's filtering system	√	√	√		√	√	√	√	√
Accidentally accessing offensive or pornographic material and failing to report the incident	√	√	√		√	√	√	√	
Deliberately accessing or trying to access offensive or pornographic material	√	√	√	√	√	√	√	√	√

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	√	√	√	√	√	√	√	√
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	√	√						
Unauthorised downloading or uploading of files	√	√				√		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	√	√			√	√		
Careless use of personal data eg holding or transferring data in an insecure manner	√	√				√		
Deliberate actions to breach data protection or network security rules	√	√	√		√	√	√	√
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	√	√	√		√	√	√	√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√		√	√	√	√
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	√	√	√			√	√	
Actions which could compromise the staff member's professional standing	√	√	√			√	√	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√	√		√	√	√	√
Using proxy sites or other means to subvert the school's filtering system	√	√	√		√	√	√	
Accidentally accessing offensive or pornographic	√	√	√		√	√	√	√

material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material	√	√	√	√	√	√	√	√
Breaching copyright or licensing regulations	√	√	√			√	√	
Continued infringements of the above, following previous warnings or sanctions	√	√	√	√	√	√	√	√

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Agreed at a meeting of the Full Governing Body on 19 June 2013.

Signed …… (Chair) …… (Date)

Signed ……..(Head Teacher) ……(Date)