CHILTERN PRIMARY SCHOOL

E-SAFETY POLICY

1 Introduction

This acceptable use policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults and children within the school. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate development within ICT. At present the Internet technologies used extensively by young people in both home and school environments include:

- Websites
- Social Networking and Chat Rooms
- Gaming
- Music Downloading
- Mobile phones with wireless connectivity
- Email and Instant Messaging
- Learning Platforms
- Video Broadcasting

Despite there being significant educational and social benefits associated with the use of these technologies, there are risks which need to be emphasised to all users and steps taken to safeguard against them. The policy also provides support and guidance to parents/carers and the wider community for the safe and responsible use of these technologies beyond the school. It explains procedures for any unacceptable use of these technologies by adults, children or young people.
The use of the Internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies.

The risks include:
- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- Sexting - the sending of indecent personal images, videos or text via mobile phones for private viewing. Can potentially be widely distributed and publicly viewed.
- On-line content which is abusive or pornographic

It is also important that adults are clear about the procedures, for example, only contacting children about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst the school or setting should acknowledge that every effort will be made to safeguard against all risks, it is likely that they will never be able to completely eliminate them. Any incidents that may arise should be dealt with quickly and according to policy to ensure children continue to be protected.

As part of the Every Child Matters agenda set out by the Government, the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children are protected from potential harm both within and beyond the school environment. Therefore, the involvement of children and parent/carers is also vital to the successful use of on-line technologies. This policy aims to explain how they can be a part of these safeguarding procedures. It also informs as to how children are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

Aims

- To emphasise the need to educate staff, children about the pros and cons of using new technologies both within and outside school or other educational settings.
- To provide safeguards and rules for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

2 Roles and Responsibilities of the School

2.1 Governors and Head Teacher

It is the overall responsibility of the head teacher, with the governors, to ensure that there is an overview of e-safety (as part of the wider remit of child protection) across the school with further responsibilities as follows:

- The head teacher has designated an e-safety leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of who holds this post within the school. This role will normally be part of the brief of the school's ICT co-ordinator, or the head teacher where this post is vacant.
- The head teacher, along with the governors, will need to decide if there should be a standard disclaimer on all e-mails stating that the views expressed are not necessarily those of the school or the LA. The school's policy is not to include such a disclaimer.
- Time and resources will be provided for the e-safety leader and staff to be trained and update policies, where appropriate.
- The head teacher is responsible for promoting e-safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The designated staff governor should inform governors at curriculum meetings about the progress of or any updates to the e-safety curriculum (via PSHE or ICT) and ensure governors know how this relates to child protection. At full governor meetings, all governors are to be made aware of e-safety developments from the curriculum meetings.
- Governors will ensure child protection is covered with an awareness of e-safety and how it is being addressed within the school, as it is the responsibility of governors to ensure that all child protection guidance and practices are embedded.
- An e-safety governor (who will ideally be the same person as the ICT or child protection governor) ought to challenge the school about having an AUP with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including challenging the school about having:
    - Firewalls
    - Anti-virus and anti-spyware software
    - Filters
    - Using an accredited ISP (Internet Service Provider)
    - Awareness of wireless technology issues
    - A clear policy on using personal devices.

The e-safety governor will also ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures (see the Allegation Procedure – Section 12 of Local Safeguarding Children's Board Northamptonshire) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers.

2.2 The E-Safety Leader

It is the role of the designated e-safety leader to

- appreciate the importance of e-safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff
- establish and maintain a safe ICT learning environment within the school

- ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach e-safety and for parents to feel informed and know where to go for advice
- ensure that filtering is set to the correct level for staff, children, in the initial set up of a network, stand-alone PC, staff/children laptops and the learning platform or ensure the technician is informed and carries out work as directed
- ensure that all adults are aware of the filtering levels and why they are there to protect children.
- report issues and update the head teacher on a regular basis
- liaise with the PSHE, child protection and ICT leaders (if different) so that policies and procedures are up-to-date to take account of any emerging issues and technologies
- update staff training (all staff) according to new and emerging technologies so that the correct e-safety information can be taught or adhered to
- ensure transparent monitoring of the Internet and on-line technologies - the school will need to decide here how they wish to monitor the use of the Internet and technologies by staff and children
- keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified
- work alongside the ICT leader (if different), to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis
- ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.

2.3 Staff or Adults

It is the responsibility of all adults within the school or other setting to

- ensure that they know who the designated person for child protection is within school or other setting, so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the head teacher/safeguarding lead. In the event of an allegation made against the head teacher, the chair of governors must be informed immediately
- be familiar with behaviour, anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the head teacher/safeguarding leader immediately, who should then follow the Allegations Procedure, Section 12, LSCBN, where appropriate
- check the filters are appropriate for their children and are set at the correct level. Report any concerns about filtering levels to the e-safety leader
- alert the e-safety leader of any new or arising issues and risks that may need to be included within policies and procedures
- ensure that children are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children should know what to do in the event of an incident
- be up-to-date with e-safety knowledge that is appropriate for the age group and reinforce through the curriculum
- sign an acceptable use statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices.
- use electronic communications in an appropriate way that does not breach the Data Protection Act 1998
- remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in
- school administrative staff will need to ensure that they follow the correct procedures for any data required to be taken from the school premises
- report accidental access to inappropriate materials to the e-safety Leader and Synetrix helpdesk in order that inappropriate sites are added to the restricted list or control this with the Local Control options via your broadband connection
- use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the Internet on a regular basis, especially when not connected to the school/educational setting's network
- ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft
- report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the NCC accident/incident reporting procedure in the same way as for other non-physical assaults.

2.4 Children

Children should be:

- involved in the review of acceptable use rules through the school council or other appropriate group, in line with this policy being reviewed and updated
- responsible for following the acceptable use rules whilst within school, as agreed at the beginning of each academic year or whenever a new child attends the school or setting for the first time
- taught to use the Internet in a safe and responsible manner through ICT, PSHE or other clubs and groups
- taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

3. Appropriate and Inappropriate Use

3.1 By Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered Internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff should receive a copy of the acceptable use policy and a copy of the acceptable use rules, which then need to be signed, returned to school to keep under file with a signed copy returned to the member of staff.

The acceptable use rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use. Staff training should underpin the receipt of this policy.

When accessing the learning platform from home, the same acceptable use rules will apply. The acceptable use should be similar for staff to that of the children so that an example of good practice can be established.

Please refer to appendices for a complete list of acceptable rules for staff.

In the Event of Inappropriate Use:

If a member of staff is believed to misuse the Internet or learning platform in an abusive or illegal manner, a report must be made to the head teacher/safeguarding lead immediately and then the Allegations Procedure (Section 12, LSCBN) and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

3.2 By Children or Young People

Acceptable use rules and the letter for children, young people and parents/carers are outlined in the appendices. These detail how children are expected to use the Internet and other technologies within school or other settings, including downloading or printing of any materials. The rules are there for children to understand what is expected of their behaviour and attitude when using the Internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The rules should be on display within the classrooms and computer suite, where this may be applicable.

The school will encourage parents/carers to support the rules with their child or young person. The rules will be available via the school prospectus or the school website.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means on-line should be appropriate and be copyright free when using the learning platform in or beyond school.

From time to time, the school council may be actively involved in discussing the acceptable use of technologies and the rules for misusing them.

In the Event of Inappropriate Use:
Should a child or young person be found to misuse the on-line facilities whilst at school, the consequences should occur:

- Any child found to be misusing the Internet by not following the Acceptable Use Rules may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules may result in not being allowed to access the Internet for a period of time and another letter will be sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person accidentally accesses inappropriate materials the child should report turn off the monitor and report this to an adult immediately.

Children should be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this may have legal implications.

4 The curriculum and Tools for Learning

4.1 Internet Use

We will teach children how to use the Internet safely and responsibly. They will also be taught, through ICT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should have been learnt by the time they leave Year 6:

- Internet literacy
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading information – know what is safe to upload and not upload personal information
- where to go for advice and how to report abuse

The NCC Primary ICT Scheme of Work is used to teach Internet and e-mail lessons from years 1 to 6.

These skills and competencies are taught within the curriculum so that children have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Children should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have accidentally accessed something.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address
- clubs attended and where
- names of parents
- routes to and from school
- identifying information, e.g. I am number 8 in the Youth Football Team

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded. Images of children should be stored according to policy.

4.2 Pupils with Additional Learning Needs

The school or setting should strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and Internet access.

4.3 Learning Platform

The Northants learning platform provides a wealth of opportunity for adults, children within and beyond school to:

- access resources via the National Education Network (NEN) which extends regionally to support schools who collaborate and share work via web cams and uploading
- ask questions
- debate issues
- dialogue with peers
- dialogue with family members or carers
- access resources in real time
- access other people and cultures in real time
- develop an on-line community

The tools available for use within the learning platform for adults, children include:

- Internet access
- E-mail
- Video-conferencing
- Weblogs (on-line diaries)
- Wikis (on-line encyclopaedia or dictionary)
- Instant Messaging .
- An on-line personal space for adapting as a user to:
    - upload work
    - access calendars and diaries
    - blog

The personal space (MySite) is designed to provide young users with the facility to share information and work collaboratively with others members of the Northamptonshire enable community. It should be noted that MySite provides the user with a private area where they may store information about themselves, accessible only to other platform users via an 'invite' system. Before students access and populate this area, guidance and support should be given to young people regarding the appropriate use of personal details on social networking sites (such as Facebook and Bebo) and how to keep themselves safe whilst online.

Children should use their login and password to access the Internet via the learning platform so that the level of filtering is appropriate. Staff should be ensuring that children are not bypassing the login to get to the learning platform so that they are protected to the best of the school's ability, in line with the embc-pl AUP and NCC policy.

Staff or adults need to ensure they consider the risks and consequences of anything they or their children may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

4.4 E-mail Use

The school will provide e-mail addresses for children to use, as a class and/or as individuals as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

Individual email accounts can be traced if there is an incident of misuse whereas class email accounts cannot, especially for older users.

Staff and children should use their school issued email addresses for any communication between home and school only. A breach of this may be considered a misuse.

Parents/carers are encouraged to be involved with the monitoring of emails sent, although the best approach with children is to communicate about who they may be talking to and assess risks together.

Teachers are expected to monitor their class use of emails where there are communications between home and school/setting, on a regular basis.

4.5 Mobile Telephones and Other Emerging Technologies

The school will carefully consider how the use of mobile technologies can be used as a teaching and learning tool within the curriculum with the following areas of concern to be taken into consideration:

- Inappropriate or bullying text messages.
- Images or video taken of adults or peers without permission being sought.
- 'Happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult which is often distributed.
- Sexting- the sending of suggestive or sexually explicit personal images via mobile phones.
- Wireless Internet access which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.

At present, the school does only allows pupils who travel to/from school without adult supervision to bring mobile phones to school. These must remain switched off and in the cloakroom throughout the school day.

Staff may bring in personal mobile phones or devices for their own use but they must not use personal numbers to contact children under any circumstances. In an emergency, staff may use their personal devices to contact parents.

Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras (see 7.6 for further details).

Staff should be aware that games consoles such as the Sony Playstation, Microsoft Xbox and other such systems have Internet access which may not include filtering. Before use within school, authorisation should be sought from the head teacher and the activity supervised by a member of staff at all times.

The school is not responsible for any theft, loss or damage of any personal mobile device.

4.5.1 School-issued Mobile Devices

The management of the use of these devices should be similar to those stated above, but with the following additions:
Where the establishment has provided a mobile device to a member of staff, such as a laptop, PDA or mobile phone, only this equipment should be used to conduct school business outside of the school environment. Also, this equipment should not be used for person business.

4.6 Videos and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

Generally, staff should not use their personal cameras, mobile phones or other personal equipment to take photographs or videos of children. If they do, images should be transferred to the school network at the earliest opportunity and the images deleted from the device.

Images may not be posted to weblogs, forums, social networking sites, etc.

Photographs/images used to identify children in a forum or using Instant Messaging within the learning platform should be representative of the child rather than of the child e.g. an avatar.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name although child protection guidance states either a child's name or a photograph but not both. Group photographs are preferable to individual children and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit.

4.7 Video-Conferencing and Webcams

Click2Meet is the main video conferencing service provided by EMBC which allows staff to preset a secure 'conference room' which remains under their control throughout the session. Similarly, the JANET video conferencing service can be used where high end equipment is available. The use of webcams to video-conference will be via EMBC which is a filtered service. Publicly accessible webcams are not used in school.

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school setting. This process should always supervised by a member of staff.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the acceptable use rules.)

Where children, young people (or adults) may be using a webcam in a family area at home as part of a school-based project, they should have open communications with parents/carers about their use and adhere to the acceptable use rules.

5 Web 2.0 Technologies

5.1 Managing Social Networking and Other Web 2.0 Technologies

Social networking sites have emerged in recent years as a leading method of communication, proving increasingly popular amongst both adults and young people alike. The service typically offers users both a public and private space through which they can engage with other online users, and express themselves creatively through images, web content and their own personal profile page. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with children, there are a number of risks associated which must be addressed. With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, MySpace and Bebo.)

In response to this issue the following measures are in force:

- The school controls access to social networking sites through existing filtering systems and only permits the use of approved sites via the LP+ learning platform. Access to public forums such as Facebook is not permitted.

- Children will be advised against giving out personal details or information which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, personal email address or full names of friends.)
- Children will only be permitted to post personal photos once communication is well established via a bona fide educational organisation, and where the supervising teacher is confident that the other organisation has robust e-safety procedures in place. .

The school/educational setting should be aware that social networking can be a vehicle for cyber-bullying. Pupils are encouraged to report any incidents of bullying to the school allowing for the procedures, as set out in the anti-bullying policy, to be followed.

5.2 Social Networking Advice for Staff

Social networking outside of work hours, on non school-issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in online contact with students other than through the school's learning platform (LP+) system.
- Staff should ensure that full privacy settings are in place on any personal social networking sites to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students)

There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a professional level. Some schools and other educational settings have set up accounts on Facebook to manage and monitor public and pupil communications through designated members of staff. Other such professional social networking tools include EdModo or virtual learning environments such as Moodle which contain similar features. However, such approaches are not authorised at our school.

6 Safeguarding Measures

6.1 Filtering

Please refer to the acceptable use rules for staff and children for the appropriate use of the learning platform.

The EMBC broadband connectivity has a filter system which is set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. All filtering should be set to 'no access' within any setting and then controlled via portal control (controls filtering at local site level) which controls individual access to the Internet. This also links to the EMBC-pl criteria 'Schedule 11' of level four site filtering to qualify for access to the broadband services.

The head teacher has signed an agreement to the filtering levels being maintained as part of the connectivity to broadband requirements from embc-pl. met. This complies with the agreed connectivity legalities with Synetrix and EMBC-pl and also ensures our younger audiences are not exposed to unnecessary risks e.g. a blanket level two for primary school users, is inappropriate.

The learning platform is set within a filtering service that will provide the same level of protection for all users.

Anti-virus and anti-spyware software is used on all network and standalone PCs or laptops and is updated on a regular basis.

A firewall ensures information about children and the school cannot be accessed by unauthorised users.

The ‘skin’ of the on-line personal space is age appropriate and only tools appropriate to the age of the child are available.

An RSS (Really Simple Syndication) feed provides a direct link to commonly used websites so that children do not need to leave their personal space for updates.

Children should use a search engine that is age appropriate such as AskJeeveskids or Yahooligans. Alternatively, they may use a general search engine such as Google providing they do so under adult supervision at all times.

CEOP (Child Exploitation and On-line Protection Centre) training for Year 6 Primary children is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible. A link to the www.thinkuknow.co.uk website is part of the skin layout for further advice and information on children’s or young people’s personal on line spaces.

6.2 Tools for Bypassing Filtering

Students and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school or educational setting’s security controls (including Internet filters, antivirus solutions or firewalls.) as stated in the Acceptable Use Rules. Violation of this rule should result in disciplinary or in some circumstances legal action. Please refer to the ‘Staff Procedures Following Misuse by Staff/Children’ sections of this document.

7 Monitoring

Teachers should monitor the use of the learning platform and Internet during lessons and also monitor the use of communications made via the school’s learning platform on a regular basis.

8 School Library

The networked computer in the school library is protected in line with the school network. The book-issue computer is password protected so that children are only able to access the system as a user.

9 Parents

9.1 Roles

Each child will be given a copy of the acceptable use rules when they first start to use on-line resources in school with any degree of independence. The AURs need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.

It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

The school will keep a record of the signed forms.

Children will not be excluded from participating in ICT activities if their parents/carers have failed to ensure the return of a signed form. However, the activities of any such children will be monitored carefully, and some restrictions may be made to their ICT access.

9.2 Support

As part of the approach to developing e-safety awareness with children, the school will provide parents with the opportunity to find out more about how they can support the school or setting in keeping their child safe and find out what they can do to continue to keep them safe whilst using on-line technologies beyond school.

We will hold an annual parent/carer information evenings and responsibility for this is part of the extended schools co-ordinator’s brief. We will also guide parents towards the Childnet International ‘KnowITAll for Parents’ CD/on-line materials (http://www.childnet-int.org.uk/kia/parents/cd/) to deliver key messages and raise awareness for parents/carers and the community.

10 Links to Other Policies

10.1 Behaviour and Anti-Bullying Policies

Please refer to the behaviour policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all ICT and PSHE materials for children and their parents/carers. People should not treat on-line behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour.

10.2 Managing Allegations and Concerns of Abuse made Against People who Work with Children.

Please refer to the Allegation Procedure, Section 12 LSCBN, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the designated person for child protection within the school or educational setting immediately. In the event of an allegation being made against a head teacher, the chair of governors should be notified immediately.

Also, contact should be made with the managing allegations team:

- Christine Churchman- South Northants cchurchman@northamptonshire.gov.uk 01604654022
- Jill Sneddon- North Northants jsneddon@northamptonshire.gov.uk 01536533933

10.3 PSHE

The teaching and learning of e-safety should be embedded within the PSHE curriculum to ensure that the key safety messages about engaging with people are the same whether children are on or off line.

10.4 Health and Safety

Refer to the health and safety policy and procedures of the school and the County Council for information on related topics, particularly display screen equipment, home working and accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

10.5 CCTV

To comply with both the Data Protection Act 1998 and the Information Commissioner's CCTV Code of Practice, all schools using CCTV for security and safety purposes must publicly declare that they are doing so. The school should have erected a sign to inform members of the public that they are entering a surveillance area and to display the following key information.

- The name of the school/individuals responsible for the CCTV system
- The contact details of who is responsible for the system
- The purpose of the CCTV system

The school must ensure that all images recorded through the CCTV system are fully traceable with the date, time, recording device and person responsible for recording all detailed in a secure log for audit trail purposes.

At present, the school has only an 'entry camera' system which does not record images.

10.6 School Website (if different to the Learning Platform Space)

The uploading of images to the school website should be subject to the same acceptable rules as uploading to any personal on-line space. Parents are informed when their child joins the school that images of pupils may be used on the school website and that they may request that no images of their child are used in this way.

10.7 External Websites

In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, schools/settings are encouraged to report incidents to the head teacher and unions, using the reporting procedures for monitoring.

10.8 Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the governing body.

Appendix 1

Staff Procedures Following Misuse by Staff

The head teacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A An inappropriate website is accessed inadvertently

- Report website to the e-safety leader if this is deemed necessary.
- Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned or restricted list. Change local control filters to restrict locally.
- Check the filter level is at the appropriate level for staff use in school.

B An inappropriate website is accessed deliberately

- Ensure that no one else can access the material by shutting down.
- Log the incident.
- Report to the head teacher and e-safety leader immediately.
- head teacher to refer back to the acceptable use rules and follow agreed actions for discipline.
- Inform the LA/RBC filtering services as with A.

C An adult receives inappropriate material

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the head teacher immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police.

D An adult has used ICT equipment inappropriately:

- Follow the procedures for B.

E An adult has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately, if necessary.
- Report to the head teacher and designated person for child protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, LSCBN.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- Once procedures and policy have been followed and the incident is considered innocent, refer to the acceptable use rules for staff and head teacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the head teacher or chair of governors (if allegation is made against the head teacher) and designated person for child protection immediately and follow the sllegations procedure and Child Protection Policy.
- Contact CEOP (police) as necessary.

F Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:

- Preserve any evidence.
- Inform the head teacher immediately and follow Child Protection Policy as necessary.
- Inform the RBC/LA/LSCBN and e-safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

G Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the head teacher.

Appendix 2

Staff Procedures Following Misuse by Children and Young People

The head teacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A An inappropriate website is accessed inadvertently:

- Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
- Report website to the e-safety Leader if this is deemed necessary.
- Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list or use Local Control to alter within your setting.
- Check the filter level is at the appropriate level for staff use in school.

B An inappropriate website is accessed deliberately:

- Refer the child to the Acceptable Use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction.
- Notify the parent/carer.
- Inform LA/RBC as above.

C An adult or child has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately.
- Report to the head teacher and Designated Person for Child Protection immediately.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse the head teacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, LSCBN.
- Contact CEOP (police) as necessary.

D Threatening or malicious comments are posted to the school website or learning platform about a child in school:

- Preserve any evidence.
- Inform the head teacher immediately.
- Inform the RBC/LA/LSCBN and e-safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

E Threatening or malicious comments are posted on external websites about an adult in the school or setting:

- Preserve any evidence.
- Inform the head teacher immediately.

NB There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of ‘grooming’ behaviour.
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of ‘making’ an image.
www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Child Protection Policy from the Local Safeguarding Children's Board Northamptonshire guidance.
All adults should know who the designated person for child protection is.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Appendix 3

Chiltern Primary School
Acceptable Use Rules for Staff, Governors and Visitors

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or e-mail, they are asked to sign these acceptable use rules. This is so that they provide an example to children for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner.
- I understand that I need to give permission to children before they can upload images (video or photographs) to the Internet or send them via e-mail.
- I know that images should not be inappropriate or reveal any personal information of children if uploading to the Internet.
- I have read the procedures for incidents of misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the head teacher, the designated person for child protection or e-safety leader in accordance with procedures listed in the acceptable use policy.
- I know who is my designated person for child protection.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children via personal technologies, including my personal e-mail or mobile phone, and should use the school e-mail and phones (if provided) and only to a child's school e-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the head teacher and/or e-safety leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-safety leader.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass school filtering systems is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures for staff misuse.
- I have been given a copy of the acceptable use policy to refer to about all e-safety issues and procedures that I should follow.

I have read, understood and agree with these rules as I know that by following them I have a better understanding of e-safety and my responsibilities to safeguard children when using on-line technologies.

Signed…….Date…….

Name (printed)…….

Appendix 4

Chiltern Primary School
E-Safety Acceptable Use Rules Letter to Parents/Carers

Dear Parent/Guardian

E-Safety Acceptable Use Rules

As part of an enriched curriculum your child will be accessing the Internet, e-mail and personal on-line space via the East Midlands Broadband Consortium (EMBC) and the It's Learning Platform. In order to support the school in educating your child about e-safety (safe use of the Internet), please read the rules below, with your child, then sign and return the attached slip.

In the event of a breach of the rules by any child our e-safety policy lists further actions and consequences, should you wish to view it. These rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and other on-line tools (eg mobile phones), both within and beyond school.

Should you wish to discuss the matter further please contact the school office.

Key Stage 1
These are our rules for using the Internet safely.

- We will only use websites our teacher has allowed us to visit.
- We will always be polite and friendly when we send messages by e-mail to other known users.
- We will only tell people our first name when we send messages.
- We will never send messages or emails to users we don't know.
- We will only send photographs if our teacher has given us permission.
- We will keep our password a secret.
- We will tell an adult straight away if we see something on-screen we do not like.

Key Stage 2
These are our rules for using the Internet safely and responsibly.

- We will use the Internet safely and responsibly.
- We will only e-mail, chat to or video-conference people an adult has approved.
- We will only use websites our teacher has allowed us to visit.
- We will always be polite and friendly when we send messages by e-mail to other known users.
- We will never send messages or emails to users we don't know.
- We will never give out passwords or detailed personal information (like our surname, address or phone number).
- We will never upload photographs or video clips without permission and never include names with photographs.
- If we see anything on the Internet or in an e-mail that makes us uncomfortable, we will turn off the monitor and tell an adult immediately.

Chiltern Primary School

E-safety Acceptable Use Rules Return Slip

Child Agreement:

Name: _____

I understand the rules for using the Internet, e-mail and on-line tools, safely and responsibly.

I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child's Signature: _____ Date: _____

Parent/Guardian Agreement:

I have read and discussed the rules with my child and confirm that he/she has understood what the rules mean.

I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, e-mail and on-line tools. I understand that occasionally inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to the policy.

I understand that whilst my child is using the Internet, and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent/Guardian Signature _____ Print Name _____

Date: _____