Acceptable Use Policy for Schools-based Employees and pupils

1. Policy Statement

In order to create a safe teaching and learning environment, effective policies and procedures which are clearly understood and followed by the whole school community are essential. This Acceptable Use Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard adults, children and young people within a school or educational setting. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate developments within ICT. This policy explains procedures for any unacceptable or misuse of these technologies by adults or children.

Why we have an Acceptable Use Policy (AUP)?
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 use these technologies. These 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.
- On-line content which is abusive or pornographic.

Whilst the school acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will 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 vital to the successful use of online technologies. This policy aims to inform how parents/carers and children are part of the procedures and how children are educated to be safe and responsible users. The term 'e safety' is used to encompass the safe use of all on-line technologies in order to protect children and adults from potential and known risks.

The purpose of the Acceptable Use Policy is to clearly identify for the whole school community:

the steps taken in school to ensure the-Safety of pupils when using the internet, e-mail and related technologies

the school's expectations for the behaviour of the whole school community whilst using the internet, e-mail and related technologies within and beyond school

the school's expectations for the behaviour of staff when accessing and using data.

2. Scope of policy

The policy applies to all school based employees, including individuals working in a voluntary capacity. All schools are expected to ensure that non- employees on site are made aware of the expectation that technologies and the internet are used safely and appropriately. The Acceptable Use Policy should be used in conjunction with the school/educational settings' disciplinary procedures and code of conduct applicable to employees and pupils.

Where this policy is applied to the Head Teacher, the Chair of Governors will be responsible for its implementation.

Where the Governing Body wishes to deviate from this proposed policy or adopt any other policy, it is the responsibility of the Governing Body to arrange consultation with appropriate representatives from recognised trade unions and professional associations.

3. Legal background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of all school employees in relation to use of technologies feature within the following legislative documents which should be referred to for further information:

The Children Act 2004
School Staffing (England) Regulations 2009
Working Together to Safeguard Children 2010
Education Act 2002
Safeguarding Vulnerable Groups Act 2009

All safeguarding responsibilities of schools and individuals referred to within this Acceptable Use Policy includes, but is not restricted to the legislation listed above.

4. Responsibilities

Head Teacher and Governors

The Head teacher and Governors have overall responsibility for e-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the Head Teacher and Governors should:

- designate an e-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed appropriately. All employees, students and volunteers should be aware of who holds this post within school.

- provide resources and time for the e-Safety lead and employees to be trained and update protocols where appropriate.

- promote e-safety across the curriculum and have an awareness of how this is being developed, linked with the school development plan.

- share any e-safety progress and curriculum updates at all governing body meetings and ensure that all present understand the link to child protection.

- ensure that e-safety is embedded within all child protection training, guidance and practices.

- elect an e-Safety Governor to challenge the school about e-Safety issues.

- make employees aware of the LSCBN Inter-agency Child Protection Procedures at www.lscbnorthamptonshire.org.uk

E-Safety Lead

The nominated e-Safety lead should:

- recognise the importance of e-Safety and understand the school's duty of care for the-Safety of their pupils and employees.
- establish and maintain a safe ICT learning environment within the school.
- ensure that all individuals in a position of trust who access technology with students understand how filtering levels operate and their purpose.

- with the support of the Network Manager or IT Subject Leader, ensure that filtering is set to the correct level for employees, young volunteers, children and young people accessing school equipment.

- report issues of concern and update the Head Teacher on a regular basis.

- liaise with the Anti-Bullying, Child Protection and ICT leads so that procedures are updated and communicated, and take into account any emerging e-safety issues and technological changes.

- co-ordinate and deliver employee training according to new and emerging technologies so that the correct e-Safety information is being delivered.

- maintain an e-Safety Incident Log to be shared at agreed intervals with theHead Teacher and Governors at governing body meetings.

- with the support of the Network Manager or ICT Lead, implement a system of monitoring employee and pupil use of school issued technologies and the internet where appropriate (School must decide how they wish to do this-i.e. monitor upon concern raised, random monitoring through collection of devices,or purchase of specialist monitoring software e.g. Securus)

- 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.

- ensure that unsolicited e-mails to a member of staff from other sources is minimised (spam block controls) Refer to section 12 of the Allegation Procedure, LSCBN, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.

Individual Responsibilities

All school based employees, including volunteers, must:

- take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.
- ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner. Children should be informed about what to do in the event of an e-Safety incident.
- 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 Headteacher.
- ensure that children are protected and supported in their use of on-line technologies so that they know how to use them in a safe and responsible manner so that they can be in control and 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.
- use school ICT systems and resources for all school related business and communications, particularly those involving sensitive pupil data or images of students. School issued email addresses, mobile phones and cameras must always be used by employees unless specific written permission to use a personal device has been granted by the Head Teacher, for example, due to equipment shortages.
- ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with their professional role and in line with school protocols. Personal details, such as mobile number, social network details and personal e-mail should not be shared or used to communicate with pupils and their families.
- not post online any text, image, sound or video which could upset or offend any member of the whole school community or be incompatible with their professional role. Individuals working with children and young people must understand that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites.
- protect their passwords/personal logins and log-off the network wherever possible when leaving work stations unattended.
- 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 network.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies

- understand that network activity and online communications on school equipment (both within and outside of the school environment) may be monitored, including any personal use of the school network. Specific details of any monitoring activity in place, including its extent and the manner in which it is carried out, should be detailed in the school's local ICT Policy
- understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.

5. Inappropriate Use

In the event of staff misuse

If an employee is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, a report must be made to the Head teacher/Safeguarding lead immediately. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

Schools Senior HR Advisory Team
LADO (Local Authority Designated Officer) Police/CEOP
(if appropriate)

Please refer to the e Safety Incident Flowchart within the accompanying Staff Handbook for further details.

In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed only if appropriate.

Examples of inappropriate use

Accepting or requesting pupils as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers with students.

Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.

In the event of inappropriate use by a child or young person

In the event of accidental access to inappropriate materials, students are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action. Template student Acceptable Use Rules and example sanctions can be found in the appendix.

Students should recognise the CEOP Report Abuse button (www.thinkuknow.co.uk) as a place where they can make confidential reports about online abuse, sexual requests or other misuse which they feel cannot be shared with employees.

6. Policy Review

The Acceptable Use Policy will be updated to reflect any technological developments and changes to the school's ICT Infrastructure. Acceptable Use Rules for students should be consulted upon by the student body to ensure that all young people can understand and adhere to expectations for online behaviour.

7. Use of specific technologies and support

Internet use

We teach our children and young people how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through ICT where the following concepts, skills and competencies have been taught by the time they leave *Year 2*:

- Internet literacy
- making good judgements about websites
- knowledge of risks such as viruses and opening mail from a stranger
- uploading information – know what is safe to upload and not upload personal information
- where to go for advice and how to report abuse

Most pupils recognise the need to be safe and act responsibly when using digital communications. Children are taught the SEIS internet rules (these are displayed throughout the school.
The www.thinkuknow.co.uk resources will be used, with free training provided to teachers/adults for the delivery of these lessons.
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 will 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 including:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address
- school
- clubs attended and where
- age or DOB
- names of parents
- routes to and from school
- identifying information,

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.

Learning Platform

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

- 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

Whilst not used in school, the personal space contains some information about the user. This area should be used as an opportunity for parents/carers to discuss with children appropriate information to enter to **ANY** website asking for personal details (such as a social networking site SNS e.g. Bebo, My space, MSN, Twitter and Facebook) and should reflect key messages for any on-line use.
Children should use their login and password to access the Learning Platform
Staff or adults need to ensure they consider the risks and consequences of anything they 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.

E-mail use

Staff, children and young people are to use their school issued e-mail addresses for any communication between home and school only.

Parents/carers are encouraged to be involved with the monitoring of E-mails 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 E-mails where there are communications between home and school, on a regular basis.

Video-conferencing

The use of web cams to video-conference will be via the learning platform which is a filtered service.
Trained staff will supervise this at all time.
Where children and adults may be using a web cam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Rules.
Taking images via a web cam will follow the same procedures as taking images with a digital or video camera.

Mobile Phone

Staff members are not allowed to use their personal numbers to contact children under any circumstances.
It is also our policy to ensure that we educate our children in understanding the use of a public domain and the consequences of misusing it including the legal implications and law enforcement through relevant curriculum links.
Other technologies schools use with children and young people are:

- *Photocopiers*
- *fax machines*
- *telephone*

Video 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. When in school there is access to:
The personal space on the learning platform should not have personal photographs uploaded that reveal more than a general location, an activity (without close-ups of children’s faces) or piece of work, without the express permission of parents/carers and school.
It is also highly recommended that permission is sought prior to any uploading of images to check for inappropriate content.
The sharing of photographs via weblogs, forums or any other means on-line will only occur after permission has been given by a parent/carer or member of staff.
Photographs/images used to identify children in a forum or using Instant Messaging within the Learning Platform will 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 young people and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit.
Photographs will be stored carefully and are only accessible to key staff with passwords.

Filtering and safeguarding measures

Staff and children are required to use the personalised learning space and all tools within it, in an acceptable way. Please refer to the Acceptable Use Rules for Staff and children and young people for the appropriate use of the learning platform.
The broadband connectivity has a filter system which should be 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.

Support

The school will send home guidelines on the use of the internet, emails and online technology at home and at school.
They will be told about 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. This will help them find out how to use the tools their children are using.
The Appendices detail where parents/carers can go for further support beyond the school. The school will endeavour to provide access to the Internet for parents/carers so that appropriate advice and information can be accessed where there may be no Internet at home, subject to arrangement.

Useful Links

NASUWT Social Networking- Guidelines for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNet working

NUT E-Safety: Protecting School Staff- Guidance for Members
http://www.teachers.org.uk/node/12516

UNISON- Guidance on Social Networking
http://www.unison.org.uk/education/schools/pages_view.asp?did=9786

Acceptable Use Rules for staff.

Higham Ferrers Nursery and Infant School 2013.

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 and young people 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 have read and understand the SEIS acceptable use/e policy document, I understand there are procedures/sanctions in place to ensure safe online practices.
- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Internet or send them via E-mail and I know that images should not be inappropriate or reveal any personal information of children and young people 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 and I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Person for Child Protection or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I will record/report incidents of cyber bullying; reporting to the Headteacher, Designated Person for Child Protection or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Person for Child Protection is.

- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail 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 Headteacher 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 only install hardware and software I have been given permission for.
- 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 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 will adhere to copyright and intellectual property rights.
- I have received regular e safety training and information to highlight the risks to my own and pupil online safety. I know who to go to if I have any further questions.

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 and young people when using on-line technologies.

Signed………………………………………………….Date…………………….

Name (printed)…………………………………………………

School…………………………………………………………………………...

E-Safety Acceptable Use Rules Letter to Parents/Carer for Primary

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the Internet, E-mail and personal on-line space via the DB Primary learning Platform.
In order to support the school in educating your child/young person about e-Safety (safe use of the Internet), please read the following Rules with your child/young person then sign and return the slip.
In the event of a breach of the Rules by any child or young person, the 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/young person about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home).
Should you wish to discuss the matter further please contact the Headteacher.
Yours faithfully,

Mrs J Hutchinson
Headteacher

…………………………………………………………………………………………