Respect for All. Learners for Life.

Acceptable Use Policy

October 2015

Development/monitoring/review of this policy

This online safety policy has been developed by a working group made up of:

- School online safety Coordinator / Officer
- Headteacher / Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors

There will be an on-going opportunity for staff to discuss with the online safety co-ordinator any issue of online safety that concerns them.

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

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way or incidents have occurred in school.

This online safety policy was approved by staff on _____

This online safety policy was approved by the Governing Body on _____

Signed: _____

Review date: _____

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

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

- Websites
- E-mail and instant messaging
- Chat rooms and social networking
- Blogs and wikis
- Podcasting
- Video broadcasting
- Music downloading
- Gaming- Xbox, playstation, wii online etc
- Mobiles/ smart phones with text, video/web functionality
- Other mobile devices with web functionality.

We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of school and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with Lister Infant School are able to use technology in a safe and responsible manner. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors, volunteers and pupils) are inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, iPads, iPod Touches, whiteboards, digital video equipment)

Disclaimer*: Due to constant changes taking place within technology, this policy may not contain the most recent developments. We will however, endeavour to add any important issues to the policy on our website.*

Roles and responsibilities

As online safety is an important aspect of strategic leader ship within the school, the Head (**JANET DAVIES**) and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named online safety co-ordinator in our school is **RACHEL MANLEY.** All the members of the school community have been made aware of who holds this post. It is the role of the online safety co-ordinator to keep abreast of current issues and guidance through organisations such as Becta, CEOP (Child Exploitation and Online Protection) and childnet.

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

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: safeguarding, child protection, health and safety, home-school-child agreement, behaviour policy and PHSE.

An Online safety committee has been selected and will meet once a term to review and update policies/procedures and provision. This will be led by Rachel Manley, supported by Kirsty Hamilton (Deputy Head), Mr S Pritchard (Governor) and Peter Davies (School Technician).

Education and training

As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. The school is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology. The school have designed an E-safety curriculum that meets the needs of all pupils and ensure their safety and well-being. The curriculum is reviewed and revised on a regular basis to ensure that it remains current. The school will also endeavour to provide information and training opportunities for parents and carers to raise their awareness of the technologies that their children are potential using and the risks that they potentially face.

Skills and development for staff and support staff
Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices, attending whole school training (Paul Bradshaw July 2015)

- They have read, understood and signed the Staff Acceptable Use Agreement.
- They report any suspected misuse or problem to the Headteacher/ online safety Coordinator/Designated Senior Person for investigation/action/sanction.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities.
- Where internet use is pre-planned puipls 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 should act as good role models in their use of digital technologies the internet and mobile devices

Managing the schools online safety messages

- We endeavour to embed online safety messages across the curriculum whenever the Internet and/or related technologies are used. online safety has been included in Health week this year (October 2015). All year groups took part in workshops on Safer Internet Day (February 2015).
- The online safety policy is introduced to the pupils at the start of each school year and pupils sign their name to agree the rules.
- online safety display (posters and top tips), Internet guidelines by each computer, details for parents on the website, guidelines for e-safety sent home with acceptable use policy.

Online safety in the curriculum

- Every year the school celebrates National Safer Internet Day, teaching the children the advantages and disadvantages of working on line and how to stay safe through simplonline safetymessages/themes.
- The school provides opportunities within a range of curriculum areas to teach about online safety, especially PHSE and Computing.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the online safety curriculum.

- Pupils are taught about respecting other people's information, images etc through discussion and modelling.
- Pupils are aware of the impact of on-line bullying and know how to seek help if they are affected by these issues. Pupils are also aware where to seek advice or help if they experience problems when using the internet and related technologies i.e. parent/carer/teacher/trusted staff member or an organisation such as childline/CEOP report abuse button.

Password security

- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems including ensuring that passwords are not shared and are changed periodically. Passwords should be on iPads, laptops and memory pens holding confidential data.
- Staff are not save passwords or ask computers to remember passwords.

Data Security and Protection

The accessing of the school data is something that the school takes very seriously. The school follows the Becta guidelines (published Autumn 2008)

All school staff will ensure that:

- Care is taken to ensure the safe keeping of data, minimising the risk of its loss or misuse.
- Data is used or processed on only secure password protected computers and other devices and that these devices are properly "logged-off" at the end of any session in which they are using personal data.
- Data is transferred securely using encryption and secure password protected devices and email solutions.

Encrypted USB sticks:

- the device **must** be password protected
- the data must be securely deleted from the device once it has been transferred or its use is complete

Managing the Internet

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Internet is logged on the server and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- Students will have supervised access to the Internet resources through the school's internet technology.
- Staff will preview any recommended sites before use.
- Image searches are discouraged when working with pupils.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other resources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- Liverpool has a monitoring solution where web based activity is monitored and recorded.
- School internet access is controlled through Liverpool Education Authority web filtering service.
- Our school has the facility for additional web filtering which is the responsibility of the E-safety co-ordinator.
- Lister Infants is aware of its responsibility when monitoring staff communication under current legislation and takes in to account: Data Protection act 1998, the telecommunications (lawful business practice) Interception of Communications regulations 2000, Regulation of Investigatory Power Acts 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based e-mail and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- If staff or pupils discover an unsuitable site, the screen must be switched off, the computer isolated and the incident reported immediately to the teacher and

then to the online safety co-ordinator/Head. A log sheet must also be completed by the member of staff.

- It is the responsibility of the school, the network technician to ensure that anti-virus is up to date on all computers and staff laptops. This automatically updates.
- Staff using personal removable media is responsible for measures to protect against viruses, for example making sure that additional systems used have up to date virus protection software. It is not the school's responsibility to install or maintain anti-virus on personal systems.
- Pupils and staff are not allowed to download programs or files on school based technologies.
- If there are any issues related to viruses or anti virus, the Computing and online safety co-ordinator should be informed.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as iPads, iPod Touches, portable media players, PDA's, gaming device, mobile and smart phones are familiar to children outside of school. They often provide a collaborative, well known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Teaching and Learning

Emerging technologies provide a flexible solution and offer a range of exciting opportunities to extend children's learning,

- Parents and children agree to and sign acceptable use agreement and will return to class teacher.
- All staff share iPad rules with children and they are displayed in all classrooms.
- School use of mobile devices, including laptops, mobile phones, cameras, iPads and iPod Touches are more commonplace and are essential elements of learning in our school.

- Children will use a range of age appropriate apps (Interactive, reference and productivity) within lessons.

- iPads and iPod Touches have Internet access which include filtering. Staff are aware of in app purchases and monitoring will take place when technologies are in use.

- Children are taught to act safely and responsibly when using technology both within, and outside of, the school environment.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

- Staff may use mobile phones during breaktimes when there are no children around. Visitors can only use mobile phones in the staffroom or office. Visitors must read and sign acceptable use before entering the school.

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

- The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

- Users bringing personal devices in to school must ensure there is no appropriate or illegal content on the device.

- Permission must be sought from the Head if a child requires a mobile phone in school. This must be taken to the office before registration and collected at hometime.

School provided Mobile devices

- The school provide staff with two mobile phones for all educational trips or visits. Group leaders can communicate with school in the event of an emergency or difficulty.

- The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

- Where the school provides mobile technologies such as laptops, cameras, video cameras etc for offsite visits and trips only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school. They are not to be used children in school.

Managing E-mail

The use of E-mail within most schools is an essential means of communication for staff and pupils. In the context of school, E-mail should not be considered private. Educationally, E-mail can offer significant be benefits including; direct written contact between schools on different projects, staff based and pupil based (overseen by adults). Staff write E-mails with the children to model good 'nettiquette'.

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored
- The school gives all staff their own E-mail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious E-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the online safety and security of users and recipients, all mail is filtered and logged, if necessary E-mail histories can be traced. This is the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal E-mail addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending e-mails to external organisations, parents or pupils are advised to cc the Headteacher.
- All Email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in Email communication, or arrange to meet anyone without specific permission and virus checking attachments.
- Offensive Emails should be reported immediately. Staff inform online safety co-ord/Head.
- Pupils are introduced to email as whole class and are taught about appropriate use and what to do if they receive an offensive email.

Safe use of Images

Taking of images and video

Digital images are easy to capture, reproduce and publish and therefore misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public without first seeking consent and understanding appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are permitted to take digital images and video 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. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

Consent of the adults who work at the school

- Permission to use images of all staff who work at the school is sought on induction and on the staff acceptable use form.

Publishing pupils images and work

Every school year, as part of the acceptable use agreement all parents/guardians will be asked to give permission to us their child's work/photographs in the following ways:

- On the school website.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- In display material that may be used in the school's communal areas and in external areas i.e. exhibition promoting the school.
- General media appearances.

This consent form is considered valid for the entire year unless there is a change in the child's circumstances.

Parents/Carers may withdraw permission, in writing, at any time.

Pupils names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published. Once

photographs and class information/celebrations have been authorised by the Head/Senior Management Team, staff have authority to upload to the site (including Admin Officer).

Storage of images

- Images /videos of the children are stored on the server.
- Pupils and staff are not permitted to use personal portable media for storage of images without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the network.
- Images are regularly monitored and deleted during staff meetings.

Webcams

We do not use webcams within school.

Misuse and Infringements

Complaints

Complaints relating to online safety should be made to the online safety co-ordinator or Headteacher. Incidents should be logged and the flowchart for managing an E- safety incident should be followed (see appendix)

Unsuitable/ Inappropriate material

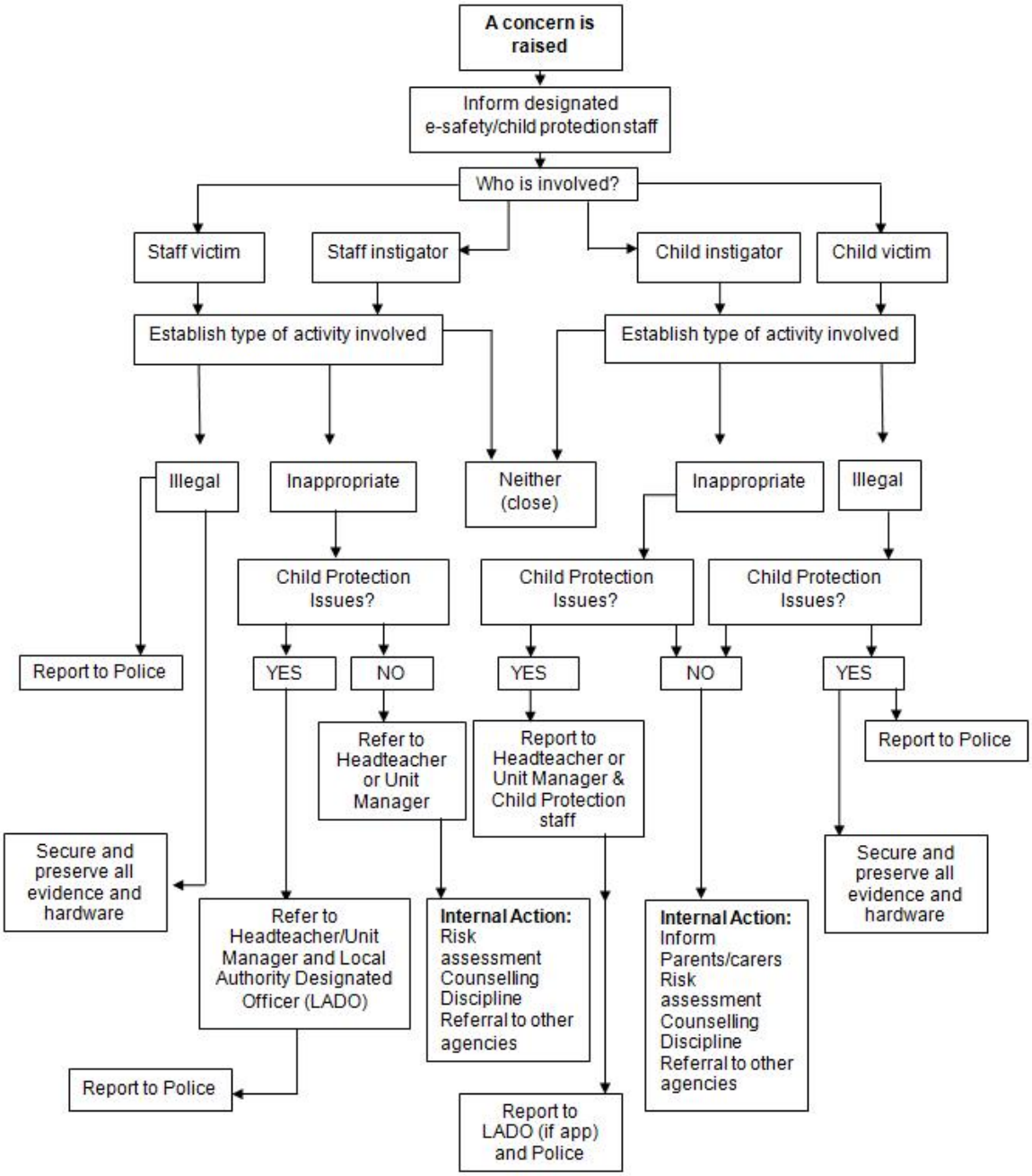
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be reported to the online safety co-ordinator/Head.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-safety co-ordinator, depending on the seriousness of the offence: investigation by the Head/LEA, immediate suspensions, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct on the Acceptable Use Agreement.

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 accidently, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of an online safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the incident flowchart below



Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's online safety rules.

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

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

Parental Involvement

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site
- Parents/Carers sessions
- High profile events/campaigns e.g. Safer Internet Day
- Parents/carers and pupils are actively encouraged to contribute to the school online safety policy by letter and by reporting unsuitable sites etc to the online safety co-ordinator.
- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (school website/media etc)

Appendix

Acceptable Use Agreement/Code of conduct: Staff and Governors

ICT and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Rachel Manley, the school's E-safety co-ordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online safety co-ordinator, depending on the seriousness of the offence; investigation by the Head Teacher/LEA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

- I will support and promote the school's online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will report and incidents of concern regarding children's safety to the designated Child Protection Co-ordinator. (Janet Davies)
- I will only use the approved, secure email system(s) for any school business.
- I understand that it is a criminal offence to use the school ICT system for purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras; email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that the school information systems may not be used for private purposes without specific permission from the Head Teacher.
- I understand that my use of school information systems, laptops, iPads, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any hardware or software without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher
- I will respect copyright and intellectual property.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signature:..... Date:.....

Full name (printed)..... Job title:.....

Acceptable Use Agreement/Code of conduct: Visitors

ICT and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all visitors are aware of their professional responsibilities when using any form of ICT within school. All visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Rachel Manley, the school's online safety co-ordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-safety co-ordinator, depending on the seriousness of the offence; investigation by the Head teacher/LEA, immediate suspension, possibly leading to the involvement of police for very serious offences.

- I will not give out my personal details, such as mobile phone numbers and personal e-mail address to pupils.
- I will only use my mobile phone in the designated areas (staffroom/office).

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature:..... Date:.....
Full name (printed)..... Job title:.....

Abbreviations

ICT- Information, Communications Technology.

Becta,- British Educational Communications and Technology Agency

CEOP -Child Exploitation and Online Protection

PHSE- personal ,health and social education

MIS system- Management Information System(s). (admin computer with pupil data)

PDA's- Personal Digital Assistant

LEA- local education authority