E Safety Policy

2016

Signed (Chair of Governors)……

Signed (Head teacher)……

Date……

Review Date……

This Policy complies with Warrington LA guidance.	**YES**
This Policy will be reviewed in	**2018**
The Policy was agreed by Governors in:	**2015**
The Policy is available for staff at:	**Staffroom**
And for parents/carers at:	**NA**

Introduction

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, Latchford St James CE Primary School endeavours to harness the potential of these technologies in order to arm our young people with the knowledge, skills and attitudes to become safe and able users of ICT.

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

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

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, can potentially be harmful for children in certain circumstances. However, we have robust systems in place that draw our attention to any potential concerns if they arise. Cases of inappropriate or dangerous use of ICT are identified by our monitoring software and logged. If necessary, parents are informed and children taught how to avoid problems in the future.

We understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets,

webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises utilising the school's network (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named E-Safety co-ordinator in our school is **Martin Flute**. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Warrington LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head or E-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 (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE.

E-Safety skills development for staff

Our staff regularly receive information and training on E-Safety issues in the form of regular staff training.

Details of the ongoing staff training programme can be found in the School Improvement Plan (SIP).

New staff receive information on the school's acceptable use policy as part of their induction.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)

All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

Managing the school E-Safety messages

We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.

The E-Safety policy will be introduced to the pupils at the start of each school year.

E-safety posters will be prominently displayed.

E-Safety in the Curriculum
Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/CEOP report abuse button.

Password Security
All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.

Users are provided with an individual network, email log-in username.

Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS MIS system and/or Virtual Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. Children are not allowed to browse the internet unsupervised.

Data Security
The accessing of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008). Staff are aware of their responsibility when accessing school data. They must not;

- allow others to view the data
- edit the data unless specifically requested to do so by the Headteacher.

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.

Use of ICT in school is logged and the logs are randomly monitored. Whenever any inappropriate use is detected it will be followed up by Warrington Borough Council and/ or the school through its E-Safety responsibilities.
Pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.

Staff will preview any recommended sites before use.

Raw image searches are not allowed when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

INFRASTRUCTURE

Warrington Local Authority has a monitoring solution where web-based activity is monitored and recorded. Inappropriate websites are blocked to protect children from inappropriate content.
School internet access is controlled through the LA's schools web filtering service.

The school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

The school uses management control tools for controlling and monitoring workstations.

If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator.

It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.

Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher.

At present, the school denies access to social networking sites to pupils within school. It is also noted that the age of the children would suggest that they are too young to sign up to many of the most popular social networking sites but may have access to them at home. Therefore all the advice and teaching is given in context of being SMART on line. All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.

Our pupils are asked to report any incidents of bullying to the school.

Staff may only create blogs, wikis or other web spaces in order to communicate with pupils using the systems approved by the Headteacher.

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 portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. 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.

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.

Pupils are not allowed to bring personal mobile devices/phones to school unless with the prior approval of the school.

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

The sending of inappropriate text messages or emails 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 into school must ensure there is no inappropriate or illegal content on the device.

Staff should not contact pupils outside normal school hours.

School provided Mobile devices (including phones)

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

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

Where the school provides mobile technologies such as phones, laptops and PDAs 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.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good ‘netiquette’.

The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

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

Under no circumstances should staff contact pupils, parents or conduct any school business using personal email 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 emails to parents should forward them to the office so that individual teacher's email addresses are protected.

Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

The forwarding of chain letters this includes jokes and funny statements is not permitted in school.

All e-mail 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 e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.

Staff must inform (the E-Safety co-ordinator/ line manager) if they receive an offensive e-mail.

Pupils are introduced to email as part of the ICT Scheme of Work.

Safe Use of Images - Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, potentially 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 considering the 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 not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. 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.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

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

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

.

Storage of Images

Images/ films of children are stored on the school's network

Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) 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 school network/ Learning Platform.

The IT coordinator has the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Webcams and CCTV

We do not use publicly accessible webcams in school.

Webcams in school will only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.

Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

Video Conferencing

Permission is sought from parents and carers if their children are involved in video conferences.

Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.

All pupils are supervised by a member of staff when video conferencing. All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.

The school will keep a record of video conferences, including date, time and participants.

Approval from the Headteacher is sought prior to all video conferences within school. The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.

No part of any video conference is recorded in any medium without the written consent of those taking part.

Complaints
Complaints relating to E-Safety should be made to the E-Safety co-ordinator or Headteacher. Incidents should be logged.

Inappropriate material
All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-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 Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Users are made aware of sanctions relating to the misuse or misconduct by formal interview and follow up letter from the Headteacher.

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 schools' E-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 has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children.

Parental Involvement
Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website).

The school disseminates information to parents relating to E-Safety where appropriate in the form of;

- E-Safety talks
- Posters
- Website postings
- Newsletter items

Writing and Reviewing this Policy
Review Procedure
There will be an on-going opportunity for staff to discuss with the E-Safety coordinator any issue of E-Safety that concerns them.
This policy will be reviewed at least every three years 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.

School …….Latchford St JamesPrimary School

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, 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 the school E-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head.
- I will not install any hardware or software without permission of the head teacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

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

Signature …….…… Date ……

Full Name ……..(printed)

School……

Job title . . . . . .

School Latchford St James CE Primary School…….

Primary Pupil Acceptable Use Agreement / E-Safety Rules (From Year Two)

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my class email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-Safety.

School …….
Dear Parent/ Carer
ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT. Please read and discuss these E-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact ……..
✂
Parent/ carer signature
We have discussed this and …….....(child name) agrees to follow the E-Safety rules and to support the safe use of ICT at Latchford St James School.
Parent/ Carer Signature ……..…….……
Class ……. Date ……

School……..

Acceptable Use Agreement:

Dear Parent/ Carer

ICT including the internet, learning platforms, email and mobile technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of E-Safety and know how to stay safe when using any ICT. Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or ……, school E-Safety coordinator.

Please return the bottom section of this form to school for filing.

✂

Pupil and Parent/ carer signature

We have discussed this document and …….....(pupil name) agrees to follow the E-Safety rules and to support the safe and responsible use of ICT at ……. School.

Parent/Carer Signature …….……

Pupil Signature…….

Form …… Date ……