New Invention Infant School

Computing Policy including E-Safety

Policy written by: Mr A Craig
Approved by the Governing Body: 17.10.2016
Date to be reviewed: Autumn 2017
School/Setting Data Controller: Mr A Craig
School/Setting Designated Child Protection Coordinator: Mrs D Naffati
School/Setting e-Safety Coordinator: Mrs L Westbury
Governor with lead responsibility: Mr J Haldron

Introduction

This policy document sets out the schools aims, principles and strategies for the delivery of the computing curriculum and keeping children safe in this technological age.

The subject is an important curriculum requirement because the ability to use computers effectively is a vital skill in modern society. The policy takes into account equipment that allows the user to communicate or handle information electronically.

Within our school this includes the use of computers, handheld devices, programmable toys, calculators, multimedia resources, virtual learning platform and listening stations. This document relates to current practice and plans for further development.

General Aims

Our aims are that

- we meet the requirements of the EYFS and National Curriculum as fully as possible
- we help all children to achieve high standards throughout the Early Years and KS 1
- we nurture social skills through collaborative group work.
- children can engage in the computing curriculum independently and tackle applications with confidence and a sense of achievement
- children develop practical skills in the computing curriculum and the ability to apply these skills to solving relevant and worthwhile problems across the whole curriculum
- children understand the capabilities and limitations of using computers and implications and consequences of their use

The Schools Approach to the computing curriculum

It is recognised that teaching time needs to be allocated to introducing new skills. This is incorporated in the planning of each scheme of work.

When planning work involving the computer teachers identify some activities in which the emphasis is on the development of computing capability and others in which the emphasis is on the subject which is being supported by using a computer.

The co-ordinator consults with each teacher to ensure that the programme of study will be taught.

Roles and Responsibilities

The roles and responsibilities with regard to Computing are as follows:

Headteacher:

- Ensures staff have access to hardware
- Purchases resources

Computing Co-ordinator:

- Oversees continuity between year groups
- Informs Head Teacher and Governors on progress in Computing
- Oversees equipment maintenance
- Organises and purchases resources

All Staff:

- Review the computing policy
- Assess pupils' progress
- Report faults to the Computing co-ordinator and/or ICT team
- Report to Head Teacher, Computing Co-ordinator and parents on children's progress, share knowledge and ideas

Governors:

- Oversee pupil progress
- Oversee budget issues
- Monitor school policy and compliance
- Monitor e-safety

Parents:

- Report any concerns or issues to school
- Informed about their children's progress

E-Safety Co-ordinator:

- Oversee acceptable use
- Liaise with Safeguarding lead

Resources

Deployment of hardware is determined through discussion with all the staff.

Nursery	Interactive Whiteboard, 1 desktop computer, 1 touch table, 2 iPads, 3 Teachers iPads, Apple TV
Reception	1 interactive whiteboard, projector, 1 laptop computer, 1touch table. 2 teacher iPads (in each classroom) To share 6 reception iPads and 6 laptop computers kept in the server room. Apple TV
Year 1	1 Clever Touch and 10 laptop computers, 8 iPods, 1 teacher iPad (in each classroom) 20 iPads to share Apple TV
Year 2 (in each classroom)	1 Clever Touch, 9 laptop computers. 8 iPods, 1 teacher iPad (in each classroom) 20 iPads to share Apple TV
Laptop bank	6 reception laptops, 1 mac-mini
Hall	1 laptop computer, sympodium, projector, DVD and video recorder, CD player and microphones

The serial numbers of all computers and iPads are held on the school inventory.
Teachers should notify the technician of all software purchased to be installed on school equipment.
All staff are aware of data protection issues (appendix)
Every classroom has wireless internet access.

All hardware/software faults should be reported to the ICT co-ordinator and recorded on the appropriate online form found in the shared area of the school network.

Recording, Assessment and Reporting

Teachers will

- monitor the use of the computers to ensure that all pupils have equal access
- track progress by using the assessment for learning records
- keep evidence of pupil work to discuss with other members of staff and as evidence for parents and interested parties

Equal Opportunities

Staff recognise that all children should have access to equipment. We will ensure this by checking:

- children in KS 1 have equal weekly access for using computers
- that when working in groups, all children have hands – on experience of the computer
- software and documentation reflect gender and ethnicity in a balanced way
- the teacher responsible for SEND and the Computing co-ordinator jointly advise teachers on the computer support which should be given to children with particular educational needs, this will include children who are gifted and talented

Health and Safety

We consider the safety and comfort of pupils and staff using computer equipment by ensuring:

- access to websites is filtered. No child is allowed to use the Internet without adult supervision. All pupils and parents must agree to the school's Acceptable Use Policy (Appendix).
- equipment is easily accessible.
- seating is adjustable
- users take frequent short breaks from computer work
- there is enough space around a workstation for paper, books and any other materials, including special educational needs equipment
- staff follow health and safety guidance regarding the height, position and distance of monitors and keyboards from pupils when working
- the school technician oversees display screen safety
- there is space for more than one pupil at a time, and for the teacher to gain access
- gangways and emergency exits are kept clear
- when working with programmable toys create a clearly defined working area to ensure that pupils do not accidentally fall over equipment
- that procedures for connecting peripherals (scanners, digital cameras, webcams, control technology/equipment and monitoring equipment), adhere to school and LA health and safety guidelines
- ensure that pupils do not take drinks to tables if they are working with electrical equipment
- in accordance with the Electricity at Work Regulations Act 1989, all electrical equipment is maintained regularly
- There is a carbon dioxide fire extinguisher available
- Care is taken to ensure that there are no trailing cables
- Children and staff are educated about the importance of e-safety

Staff INSET

INSET will be provided when staff identify needs. Training may take the form of courses offsite or the co-ordinator will conduct in house training or support.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

E-Safety depends on effective practice at a number of levels:

- Responsible computer use by all staff and students.
- Responsible mobile phone use by all staff and adults in school.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from LA Services including the effective management of filtering.
- National Education Network standards and specifications.

Why Internet use is important

- The Internet is an essential element for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils

Internet use will enhance learning

- The school internet access is designed for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

Managing Internet Access

- Information system security, school computer systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed, revised and updated where necessary with our system managers LA ICT.

E-mail

- Staff and pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published

- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Social networking and personal publishing

- The school will block access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Parents are advised that they should not post information about school, staff or children on social networking sites.
- No staff members will accept parents or children as 'friends' in any social networking site. No comments relating to school, staff or children will be posted to any social networking site.

Managing filtering

- The school will work with LA Services LTD, DFE and the Internet Service Provider and Policy Central to ensure systems to protect pupils are continually reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the named e-Safety Coordinator.
- SMT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies

- Mobile phones will be switched off at all times while children are in the building. Staff may take devices into safe areas e.g. staffroom or any school office, at break-times to switch on and make or receive personal calls. Consideration will be made if any member of staff has any emergency or safeguarding need on a case-by case basis, and steps will be taken to achieve a safe compromise for all.
- Staff with mobile devices belonging to the school need to have these switched on at all times. Their use will be monitored by the e-safety co-ordinator.
- Visitors will be reminded of the need to switch off mobile phones when they are in the building, if their stay is liable to be prolonged or unaccompanied.
- No member of the school community will be allowed to take photographs of children on their personal phones or other mobile devices.
- The sending of abusive or inappropriate text messages is forbidden.
- Video conferencing will be appropriately supervised for the pupils' age.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 (see Data Protection Policy)

Computer access

- All staff and Governors will be given the School e-Safety Policy and its importance explained
- All staff must read and sign the 'Acceptable Use Agreement' before using any school computer resources
- Pupils' access to the Internet will be under adult supervision at all times
- Everyone will be made aware that Internet traffic can be monitored and traced to the individual user
- Pupils in Key Stage 1 will be made aware of the school's e-safety rules
- Pupils will be informed that network and Internet use will be monitored
- Parents' attention will be drawn to the School e-Safety Procedures in newsletters, the school brochure and on the school Web site
- Parents will be asked to sign and return an internet access consent form
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Education Walsall can accept liability for the material accessed, or any consequences of Internet access
- Complaints of internet misuse will be dealt with by the Head Teacher and reported to LA ICT
- SMT undertake an e-Safety audit each year to assess whether the e-safety basics are in place

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not be named, be aware that children at risk will not have photographs published to protect their anonymity.
- Pupils' full names will not be used anywhere on the school website and Learning Platform particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website and Learning Platform
- Pupil's work can only be published with the permission of the pupil and parents

In addition:

- The Data Controller/DCPC and/or Management team is responsible for ensuring the acceptable, safe use and storage of all camera technology and images within the setting/school. This includes the management, implementation, monitoring and review of the School/Settings Image Use Policy.
- Written consent from parents will be kept by the setting where children's images are used for publicity purposes (such as brochures or publications), until the image is no longer in use.
- Parental permission will be sought on an agreed basis on admission to the school.
- Parental permission will be sought for all images in the case of children who are Looked After or whose family circumstances make this imperative.
- A record of all consent details will be kept securely on file. Should permission be withdrawn by parents/carers at any time, then all relevant images will be removed and disposed of and the record will be updated accordingly.
- Images will not be kept for longer than is to be considered necessary.
- All images will remain on site at all times, unless prior explicit consent has been given by both. Should permission be given to take images off site data will be kept securely (e.g. with appropriate encryption).
- The Data Controller and/or DCPC reserve the right to view any images taken and/or to withdraw or modify a member of staffs' authorisation to take or make images at any time.
- Any memory stick, CD or storage device containing images of children to be taken offsite for further work will be suitably encrypted and monitored to ensure it is returned within the expected time scale.
- Images or videos that include children will be selected carefully when used online and will not provide material that could be reused.
- Children's' full names will not be used on the website in association with photographs or work.
- The school/setting will not include any personal addresses, emails, telephone numbers, fax numbers on video, on the website, in a prospectus or in other printed publications.
- The school/setting will only use images of children who are suitably dressed.
- Children's work will only be published with their permission or their parents consent.
- Staff will receive information regarding the safe and appropriate use of images as part of their safeguarding training and responsibilities.
- All members of staff (including volunteers) will ensure that all images are available for scrutiny and will be able to justify any images in their possession.
- Any apps, websites or third party companies used to share, host or access children's images will be risk assessed prior to use. The school will ensure that images are held in accordance with the Data Protection Act and suitable child protection requirements (if necessary) are in place.
- Careful consideration is given before involving very young or vulnerable children when taking photos or recordings who may be unable to question why or how activities are taking place.
- The school/setting will discuss the use of images with children and young people in an age appropriate way.
- Images will not be taken of any child or young person against their wishes. A child or young person's right not to be photographed is to be respected.
- Photography is not permitted in sensitive areas such as changing rooms, toilets, etc.
- Photographs will be disposed of should they no longer be required. They will be returned to the parent or carer, deleted and wiped or shredded as appropriate. Copies will not to be taken of any images without relevant authority and consent from the Data Controller and/or DCPC and the parent/carer.

All images taken by the school/setting will be used in a manner respectful of the eight Data Protection Principles.

This means that images will be:

- fairly and lawfully processed
- processed for limited, specifically stated purposes only
- used in a way that is adequate, relevant and not excessive
- accurate and up to date
- kept on file for no longer than is necessary
- processed in line with an individual's legal rights
- kept securely

Clarifying School Procedures

- Any images of children captured must be taken on a school device.
- If you or the pupils use a school camera then images should be transferred directly to the school network within 1 week and deleted from the camera. All cameras should have the memory returned before returning to storage.
- If you or the children use a school iPad to capture images these must be transferred to one of the above locations within one week and images must be removed from the internal memory of these devices.
- As an iPad is an encrypted device, staff may take these home for assessment purposes whilst following the above procedures.

Use of Photos/Videos by Parents/Carers

- Parents/carers are permitted to take photographs or DVD footage of events for private use only.
- Parents/carers are only permitted to take or make recording within designated areas of the setting. Photography is not permitted in sensitive areas such as changing room, toilets, swimming areas etc.
- The opportunity for parents/carers to take photographs and make videos can be reserved by the school/setting on health and safety grounds.
- Parents and carers who are using photographic equipment must be mindful of others when making and taking images.
- The right to withdraw consent will be maintained and any photography or filming on site will be open to scrutiny at any time.
- Parents may contact the school/Data Controller/DCPC to discuss any concerns regarding the use of images.
- The setting will discuss and agree age appropriate acceptable use rules with children regarding the appropriate use of cameras, such as places children can not take the camera (e.g. unsupervised areas, toilets etc).
- All staff will be made aware of the acceptable use rules regarding children's use of cameras and will ensure that children are appropriately supervised when taking images for official or curriculum use.
- Members of staff will role model positive behaviour to the children by encouraging them to ask permission before they take any photos.
- Photos taken by children for official use will only be taken with parental consent and will be processed in accordance with the Data Protection Act 1998.
- Parents/carers will be made aware that children will be taking photos/videos of other children and will be informed how these images will be managed by the setting e.g. will be for internal use by the setting only (not shared online or via any website or social media tool).
- Photos taken by children for official use will be carefully controlled by the setting and will be checked carefully before sharing online or via digital screens.
- Still and video cameras provided for use by children and the images themselves will not be removed from the
- setting.

Use of Images of Children by the Media

- Where a press photographer is to be invited to celebrate an event, every effort will be made to ensure that the newspaper's (or other relevant media) requirements can be met. Agreement will be sought between parents and carers and the press which will request that a pre-agreed and accepted amount of personal information (e.g. first names only) can be published along with images and videos.
- The identity of any press representative will be verified and access will only be permitted where the event is planned, and where press are to be specifically invited to attend. No authorisation will be given to unscheduled visits by the press under any circumstances.
- Every effort will be made to ensure the press abide by any specific guidelines should they be requested. No responsibility or liability however can be claimed for situations beyond reasonable control, and where the school is to be considered to have acted in good faith.

Use of Professional Photographers

- Professional photographers who are engaged to record any events will be prepared to work according to the terms of the settings e-Safety policy.
- Photographers will not have unsupervised access to children and young people.
- Recordings will be retained for a limited time period only and for no longer than their intended purpose.
- Regular auditing of any stored images will be undertaken by the Data Controller and/or DCPC or other member of staff as designated by the management team.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school, building on the LSCB e-Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Acceptable Use Agreement

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password.

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy (see the image use policy) and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

- I will respect copyright and intellectual property rights and not breach LA or school policies.

- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces (See e-Safety policy). I will ensure that my personal mobile phone is turned off when children are in school.

- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator Mrs D Naffati and/or the e-Safety Coordinator Mrs L Westbury as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Mrs L. Westbury the e-Safety Coordinator.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to Mr A Craig or ICT Support as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership Team.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or Walsall LA, into disrepute.

- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator Mrs L Westbury or the Head Teacher.

- I understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance.

The School will exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: …… Print Name: …… Date: ……

Accepted by: …… Print Name: ……

Acceptable Use Policy Guidance notes for learners in KS 1

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not load photographs of myself onto the computer
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else