Sharlston School ICT and eSafety Policy Sept 16

Definition

Information and Communications Technology has the potential to improve the quality of teaching and learning across the Curriculum. Society is changing and there is an increasing need for a greater level of technological knowledge and awareness amongst the population as a whole. The effective use of ICT in the classroom will help to produce a population which feels comfortable with the new technology, is able to access lifelong learning opportunities through the use of ICT and can adapt to the rapid changes in this field.

Aims

In our school we aim to:

- ensure all staff and pupils are confident, competent and independent users of ICT
- develop an appreciation of the use of ICT in the context of the wider world
- develop pupils' ability to use ICT appropriately and choose software suitable for a particular task
- provide continuity and progression in the 2014 National Curriculum
- develop ICT and digital Literacy skills through curriculum contexts
- encourage problem-solving and investigative work

Roles and Responsibilities

The Headteacher is responsible for monitoring the teaching of ICT. The finance sub-committee ensures adequate funding is allocated to cover equipment and all necessary contracts.

The designated ICT co-ordinator will:

- oversee curriculum planning within the school
- inform the rest of the staff about new developments and, where appropriate, organise training
- share expertise and experience and advise on managing equipment and software in the classrooms but is not expected to act as technician
- maintain appropriate ICT resources and review these annually
- use the allocated budget to address whole school resource needs
- monitor teaching and learning in line with the Monitoring Programme
- periodically monitor children's files and the sites they have accessed to check the content is appropriate
- report to governors as required

All teachers are responsible for monitoring and responding to issues of e-safety and cyber bullying. Parents will be made aware of any issues arising and any sanctions which may be imposed.

Special Needs and Equal Opportunities

The school recognises the advantages of the use of ICT by pupils with special educational needs. Targets on pupil's IEPs are supported through the use of specific programs e.g. Phonics, Sumdog and Education City. In addition to this our school uses ICT to:

- address pupils' individual needs
- increase access to the curriculumation
- improve maths and literacy skills

All pupils regularly use Sumdog and Education City. Children are supplied with passwords to access these sites.

The school promotes equal opportunities for computer usage. The school monitors the level of access to computers in the home environment to ensure no pupils are unduly disadvantaged.

Software used in the school is chosen to ensure that it is non-discriminatory and promotes equal opportunities for all users.

All users of our ICT resources must agree to abide by the Acceptable Use Policy for ICT.

General

ICT is taught both as a discrete subject and integrated into all other curriculum areas. ICT is used as a tool to improve learning. The ICT Co-ordinator monitors the ICT links in the schemes of work for each subject. We aim to provide a broad and balanced curriculum through our long term plans and Rigby Star Computing yearly schemes of work.

Pupils have access to computers in their classrooms every day and each class is allocated time in the ICT suite during each week.

All the software used in school is monitored to ensure that its use is non-discriminatory and, where relevant, represents cultural diversity.

Teaching and Learning

Planning ensures that a wide range of strategies are employed in order to differentiate ICT tasks. Examples of these are:

- same activity but different outcome
- same theme but different levels of input
- different pace of working
- different groupings of pupils
- developing different modules of work, at different times of the year, for different abilities

Assessment

Clear learning objectives both in Computing and subject context will support the focus of assessed activities. The areas of Computing that have been taught each term are formally assessed and levelled and an annotated class record is kept.

Individual pupil's files are kept on the server, pupils are developing e-portfolios in their own folders and a portfolio of annotated examples of work from each class is kept.

Reporting and Recording

Parents receive an annual written report on their child's progress in Computing. In addition to this, our school provides verbal feedback on their progress during Parent interviews.

<u>E – Safety Overview</u>

The e-Safety aspects of this Policy have been written by the eSafety group, building on the LA e-Safety advice and government guidance. The eSafety group consists of the head teacher, deputy head teacher, designated safeguarding officer, ICT coordinator and eSafety governor.
This e-Safety aspects of the policy will operate in conjunction with other policies including those for ICT, Behaviour, Bullying, Curriculum, Child Protection, Data Protection and Security.
The following groups were consulted: children, teaching staff, support staff, dinner supervisors and governors.
The policy was completed Jan 2010 and was approved by the governing body on.
The policy will be reviewed annually and is due for review no later than May 2018.

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. 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 are using both inside and outside of the classroom include:

- Websites
- Learning Platforms/Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality such as tablets, Kindles and Nintendo DS

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Sharlston Community School, we understand the responsibility to educate our pupils on eSafety 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.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our school to use technology to benefit learners. Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

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 (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsiblilites

At Sharlston Community School we believe eSafety is the responsibility of the whole school community. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Management Team

- Develop and promote an eSafety culture within the school community
- Support the eSafety coordinator in their work
- Ensure that the E-Safety Coordinator and other relevant staff receive suitable CPD and have access to resources to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- Receive and regularly review eSafety incident logs and be aware of the procedure to be followed should an eSafety incident occur

Responsiblities of the ICT/E-Safety Coordinator

- Promote an awareness and commitment to eSafety throughout school
- Be the first point of contact in school on all eSafety matters
- Create and maintain policies and procedures
- Ensure all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice for staff
- Ensure eSafety is promoted with parents and carers
- Liaise with the Waterton Trust, Local Authority, MINT and other relevant agencies
- Receive reports of e-safety incidents and keep a log of incidents to inform future e-safety developments
- Monitor and report on eSafety issues to the SLT, staff or Governing Body

Responsiblities of Teachers and Support Staff

- Read, understand and help promote the eSafety policies and guidance
- Read, understand and adhere to the school staff Acceptable Use Agreement(AUP)
- Develop and maintain an awareness of current e-safety issues and guidance
- Model safe and responsible behaviours in the use of technology
- Embed eSafety issues in all aspects of the curriculum and other school activities
- Supervise pupils carefully when engaged in learning activities involving technology
- Maintain a professional level of conduct in their personal use of technology at all times and ensure any digital communications with parents and pupils (email / voice) are on a professional level and only carried out using official school systems
- Ensure that when internet use is pre-planned pupils are 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
- Be aware of what to do if an eSafety incident occurs
-

Responsibilites of Technical Staff

- Read, understand, contribute to and help promote the eSafety policies and guidance
- Read, understand and adhere to the school staff Acceptable Use Agreement(AUP)
- Support the school in providing a safe infrastructure to support learning and teaching
- Take responsibility for the security of the school ICT system ensuring that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Report any eSafety related issues to the SLT

- Develop and maintain an awareness of current e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- Liaise with the Waterton Trust and others on technical issues
- Maintain a professional level of conduct in their personal use of technology at all times and ensure any digital communications with parents and pupils are on a professional level and only carried out using official school systems

Responsibilities of Pupils

- Read, understand and follow the school pupil Acceptable Use Agreement
- Understand and follow school policies on the use of mobile phones, digital cameras and hand held devices. Know and understand school policies on the taking / use of images and on cyber-bullying
- Take responsibility for adopting good e-safety practice and learning about the benefits and risks of using the internet and other technologies in school and at home
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understand what action to take if they feel worried, uncomfortable, vulnerable or at risk whilst using technology in school or at home or if they know of someone who this is happening to
- Discuss eSafety issues with family and friends in an open and honest way

Responsibilities of Parents and Carers

- Help and support the school in promoting eSafety
- Read, understand and promote the school pupil Acceptable Use Agreement with the children
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that the children use in school and at home
- Discuss eSafety concerns with children and show an interest in how they are using the technology, encouraging them to behave sensibly and responsibly
- Consult with school if any concerns arise about children's use of technology

Responsiblities of Governing Body

- Read, understand, contribute to and help promote the school's eSafety policies and guidance
- Develop an overview of the benefits and risks of the internet and common technologies used by children
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become involved in eSafety activities

ICT and eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

In FS and KS1, eSafety education will focus on issues such as:

- Becoming aware of some of the benefits and risks of the Internet and other communication technologies, including how the Internet enables us to do many tasks in new or more efficient ways.
- Beginning to understand some of the qualities that can be used to assess if a person can be trusted, and to be aware of which adults in their lives they can safely turn to if they need help
- Identifying situations in which they should turn to a trusted adult for help

- Understanding that listening to their emotions can help them decide if a situation is unsafe
- Understanding what their personal information is, and that they should never give out their personal information online without asking a trusted adult first

KS 2 children are beginning to use the Internet and other communications technologies with greater independence. They will focus on issues such as:

- the importance of keeping personal information safe and how to deal with inappropriate internet content and contact.
- Safety training on using mobile phones to cover personal safety issues such as using a mobile phone in public, and being aware of the financial costs of using a mobile phone.
- Being aware of the impact of online bullying and know how to seek help if they are affected by these issues around Cyberbullying
- Safe Social networking sites

We hold eSafety assemblies which pupils often lead. Parents are invited to attend the assembly followed by an information meeting. We promote eSafety throughout the curriculum and also through taking part in the annual Safer Internet Day. The e-safety policy is re-introduced to the pupils at the start of each school year and children are reminded regularly about their responsibilities through the Acceptable Use Policy and also through the esafety rules which are displayed prominently throughout the school.

Managing ICT Systems and Access

School internet access is controlled through the RM's web filtering service. The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible. Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

- All internet access by pupils will be supervised closely by staff
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety officer or teacher as appropriate
- Virus protection is installed on all appropriate hardware and will be kept active and up to date by the technical staff.
- Staff using personal removable media are 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 virus protection on personal systems.

- Pupils must not bring in work on removable media to protect against viruses

- Pupils are not permitted to download programs or files on school based technologies. Staff must first seek prior permission from the ICT coordinator or technical staff

- All users will be responsible for keeping their username and passwords for ICT systems secure.

eSafety and Learning Technologies in School

Any electronic communication between staff, pupils, parents and members of the school community should be of a professional nature and related to school matters only.

Mobile Phones

The school allows staff to bring in personal mobile phones and devices for their own personal use during staff break times. These are not to be used at all during lesson times or when supervising children at break, unless special permission has been sought from the Head teacher. Under no circumstances does the school allow a member of staff to use mobile phones when supervising children and no member of staff should contact a pupil or parent/carer using their personal phone. Exceptions may take place in emergencies, on school trips and when using the school mobile phone based in the office.

E-mails

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail 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 e-mail in relation to their age and good network etiquette.

- Staff and pupils should use the approved e- mail accounts allocated to them by school and are aware that the use of the school email system is monitored and checked.

- Staff and pupils are not permitted to access personal email accounts or use the internet for personal use during school time, unless special permission has been sought from the Head teacher. Under no circumstances does the school allow a member of staff to use the internet for personal use when supervising children.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

- Any inappropriate use of the school email system or the receipt of any inappropriate messages by a user should be reported to a member of staff immediately.

Social networking sites, video conferencing and blogs, wikis ,podcasts,

- The school does not allow access to social networking sites to pupils within school

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils

- All pupils are taught to be cautious about the information given by others on any sites, for example users not being who they say they are

- Pupils are taught about the need to ensure they have maximum privacy settings on any social networking sites they may access at home

- 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

- All staff are strongly advised to ignore requests from parents and pupils to be part of their social networking site(s). Any specific personal situations will need to be brought to the attention of the Headteacher for declaration and guidance.

- Staff should regularly check their Facebooks or similar accounts for access level settings and choose the maximum privacy setting.

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

- The school keeps a record of video calls, including date, time and participants.

- Approval from the Headteacher is sought prior to all video calls within school
- Staff may only create blogs, wikis etc in order to communicate with pupils using systems approved by the Headteacher
- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils will only use regulated educational chat environments and this use will be closely supervised and the importance of chat room safety emphasised.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- A risk assessment will be carried out before pupils are allowed to use any new Learning technology in school.

<u>Publishing pupil's images and work</u>

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember and teach children 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 to support educational aims.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils unless images are transferred immediately and solely to the school's network and deleted straightaway from the personal device
- 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
- Pupils' full names will not be used anywhere on a website, or on the internet, particularly in association with photographs unless specific permission has been obtained from parents/carers
- Written permission from parents or carers will be obtained when pupils start school, to to allow photographs of pupils to be published on the school website
- Pupil's work can only be published with the permission of the pupil

<u>Data Protection</u>

- Staff must lock the screen before moving away from a computer during a normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Staff must logoff from the PC completely when going to be away from the computer for a longer period of time
- Staff must ensure that all school data is stored on school's network, and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted (USB stick)

- A time locking screensaver is applied to all machines

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, through careless or irresponsible or, very rarely, through deliberate misuse. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's eSafety Co-ordinator and/or Headteacher. Additionally, all security breaches, lost/stolen equipment or data,, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported and an incident log will be kept. All users are aware of the procedures for reporting accidental access to inappropriate materials.

Listed below are the responses that will be made to any apparent or actual incidents of misuse:

• Minor incidents

These might be incidents of misuse by pupils such as copying information into assignments and failing to acknowledge the source (plagiarism and copyright infringement); downloading materials or images not relevant to their studies; misconduct associated with student logins, such as using some one else's password because they have forgotten their own.
Many of these issues are covered within the school's acceptable use policy and in all but the most minor of cases the pupil will be issued with a warning, and the incident documented.

• Incidents involving inappropriate materials or activities

While not illegal, there will be some activities that are just not appropriate within the school environment, and, in the case of staff, not in keeping with the professional standards or code of ethics of those who work with children and young people. Incidents that involve inappropriate but legal material will be reported to the Headteacher and/or eSafety Coordinator and dealt with by the school via the usual safeguarding/disciplinary system. These are incidents which could compromise the staff member's professional standing such as using non educational internet sites or mobile phones when supervising children, inappropriate use of social networking / instant messaging / personal email in or outside of school, and the use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school. Parents will be involved if incidents outside of school become apparent that involve pupils and inappropriate internet.

• Incidents involving illegal materials or activities

If any apparent or actual misuse appears to involve illegal activity (e.g. child pornography images, adult material which potentially breaches the Obscene Publications Act, criminally racist material, extreme cyberbullying) then the concerns must be reported to the Headteacher and/or eSafety Coordinator. Such incidents will always be reported to the Waterton Trust, LA and the police. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off. Do not shut a suspect computer down as the evidence will not be preserved. After involving the police the school will then follow police recommendations. If a child is involved then the Child Protection Officer will follow the necessary procedures.

Sharlston Community School Acceptable Use Policy FS/KS1		
These rules help me to stay safe online!		
	I will only use the internet when an adult is with me	
	I only click on the buttons or links when I know what they do.	
	I can search the Internet with an adult.	
	I always use Hector to cover the page and then tell a grown up if I see something I don't like on the computer.	
	I will only write polite and friendly messages to people that I know.	
	I promise to follow these rules. My name is _______________.	

Please read, sign and date the information below to show you know how to use ICT safely and sensibly!

Sharlston Community School
Pupil Acceptable Use Agreement

□ I will only use ICT in school for school purposes.

□ I will not tell other people my passwords for learning websites.

□ I will only open/delete my own files.

□ I will make sure that all ICT related contact with other children and adults is appropriate and polite.

□ I will not deliberately look for, save or send anything that could offend others.

□ If I accidentally find anything inappropriate on the internet I will cover it with Hector and tell my teacher immediately.

□ I know not to give out my personal details such as my name, phone number, home address or school.

□ I will be responsible for my behaviour when using ICT in school or at home because I know that these rules are to keep me, and others around me, safe.

□ I will not arrange to meet anyone that I talk to online unless my parent or carer has arranged it

□ I will follow the SMART rules.

□ I know that my use of ICT can be checked and that my parent or carer will be contacted if a member of school staff is concerned about my safety.

Signature Pupil………………………………
Date ………………

Staff, Governor and Visitor Acceptable Use Agreement

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 to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this policy annually confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the Headteacher

- 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.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
- I will not use personal mobile phones when supervising children
- I will only use the school's email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school..
- I will ensure that all electronic communications with pupils parents and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number or personal email address, to pupils.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without the permission of the ICT Coordinator and Technical staff
- I will report any accidental access to inappropriate materials immediately to the eSafety Coordinator and or Headteacher
- 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 data protection 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 in line with data security policy.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the Headteacher and LA.
- I will respect copyright and intellectual property rights.

User Signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school

Signature ……………………………………………………………………………………

Date …………………… Role in School ………………………………………

Full Name ……………………………...(printed)

Please read carefully then complete. You need to photocopy the AUP to keep in your own file and then give the original to Denise

Sharlston Community School eSafety Incident Log

Details of ALL eSafety incidents will be recorded by the Head teacher or eSafety Coordinator.
This incident log will be monitored termly by the Headteacher, SMT and Chair of Governors.

Date & Time	Name of Pupil or Staff Member M/F	Room and Computer/Device Number	Details of incident (including evidence)	Actions and Reasons

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We immediately use Hector to cover any webpage we not sure about.
- We tell an adult if we see anything we are uncomfortable with.
- We only e-mail people an adult has approved.
- We send messages that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.

Think then Click

These rules help us to stay safe on the Internet

🌍	We only use the internet when an adult is with us.	
	We can click on the buttons or links when we know what they do.	🖱
🔍	We can search the Internet with an adult.	
	We always ask if we get lost on the Internet.	👣
✉	We can send and open emails together.	
	We can write polite and friendly messages to people that we know.	✓