South Hylton Primary School

Policy and Guidelines for the Acceptable Use of ICT

A. Roberts Reviewed: October 2016

Policy and Guidelines for Acceptable Use of ICT

Background

The aims of this policy are to promote the sensible and safe use of technology within school, to ensure that sensitive data is kept secure and safeguard the well being and privacy of staff and pupils.

The Acceptable use policy will operate in conjunction with other policies including those for Pupil Behaviour, Child Protection, Safeguarding and the use of ICT.

The purpose of this policy is to:

- establish the ground rules we have in South Hylton Primary School for using the Internet and electronic communications such as mobile phones and other portable ICT devices.
- ensure that sensitive data and information is not misused or unauthorized people gain access to this data.

This document applies to all users of South Hylton Primary School's system and ICT resources including student teachers, staff and parent users. It also addresses the use of the use of the property of staff and other adults in school and ICT property of the school which is used by staff for transferring information between home and school.

All technology, such as media rich phones, MP3 players, Personal Digital Assistants (PDA), memory cards, USB storage Keys, iPads and any other developing technology that can be used to store, transmit or manipulate data should be used responsibly and in accordance with these guidelines – even if not directly connected to the school network.

Logging on and Security

- Users are responsible for the protection of their own network logon accounts and should not divulge these passwords to anyone.
- Staff should ensure that no child is privy to their logon details and should logon to a system either before children are present or discreetly so that children are not aware of the logon details.
- IWB projectors should not be running when a member of staff logs onto an account.
- Users must never log on as someone else, nor use a computer which has been logged on by someone else.
- Users must log off or lock a computer when leaving a work station, even for a short time.
- Classroom computers must never be left logged on when a member of staff is not present. Staff must either log out of the system or lock a computer when leaving the room

- Computers must never be left running over break or lunchtime periods and children must never be allowed access to any computer during these periods unless directly supervised by a member of staff.

Use of the School Network and Computer Facilities

It is not acceptable for staff and other adults working within school to:

- Attempt to download or install programs to a school computer or a computer owned by the school (laptops, iPads etc.) unless agreed with the ICT Co-ordinator and checked by the ICT technician.
- Attempt to introduce a virus or malicious code deliberately.
- Attempt to bypass network and systems security.
- Attempt to gain access to another user's account.
- Attempt to use any form of hacking or cracking software.
- Connect or install a Wireless Access Point directly to the network or via a computer.
- Connect or install any form of internet access device such as modem, broadband or internet enabled mobile phones directly to the network or via a computer.
- Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence or anxiety to other users, or material which infringes copyright, or material which is unlawful.
- Engage in activities which waste technical support time or resources.
- Allow visitors i.e. supply teachers, access to the internet on their account. This must be done through the ICT co-ordinator or technician.

Use of the Internet

Access to the internet on the school network is firewalled to prevent access to inappropriate sites, and to protect the computer network and systems.

However users should be aware of the following and note that they also apply to any school property, including laptops assigned to staff for planning and preparation purposes and which are allowed off school premises:

- The use of public chat rooms or messaging services (MSN, AOL etc.) on any school owned equipment is not allowed.
- Users should not copy and use material from the Internet which breaks copyright restrictions.
- The use of the internet during school lessons is under the direction of the teacher and they are responsible for monitoring the activities of pupil.
- Users should not attempt to gain access to sites which are not directly related to school activities or to the research, planning and preparation of lessons. This includes internet shopping and personal e-mail accounts.
- Users should download any software from the internet without prior consent of the ICT co-ordinator or ICT technician.

Use of e-mail Accounts

Currently, only staff have access to e-mail accounts on the school network computers. Users need to be aware of the following restrictions:

- E-mail addresses must, under no circumstances, be shared with pupils. This applies to school e-mail accounts and personal e-mail accounts.
- Staff using Social Networking Sites on their home computers must be vigilant in keeping these details secure so no child conducting a search can access e-mail accounts.
- Private Social Networking Sites should have full privacy settings to avoid pupils/parents accessing private information such as photographs
- Pupils must never be given access to a staff's e-mail account and e-mails should not be sent on their behalf.
- Sending and receiving personal e-mails on school addresses or on school computers, including school laptops, is prohibited.
- The sending or forwarding of chain e-mails is not permitted.

Staff should also be cautious of the following and report these to the ICT co-ordinator or technician:

- Multiple e-mails from an address you don't recognize or an address that looks suspicious.
- E-mails of an offensive, insulting or pornographic nature.

Use of Instant Messaging

The use of instant messaging is not permitted within the school network or school owned property.

Use of Portable Equipment and Emerging Technologies

(*media rich phones, MP3 players, Personal Digital Assistants (PDA), memory cards, USB storage Key, iPads and any other developing technology)*

The school provides a range of portable equipment such as laptops, USB devices and digital cameras to enhance the quality of children's learning and to allow staff to provide a stimulating and motivational learning environment.

Staff are encouraged to use this equipment to enhance their planning and preparation but must be aware of the following restrictions on both school owned and personal ICT property:

- Photographs of children and personal information about children must not be taken from the school premises in electronic format i.e memory sticks or school laptops and iPads.
- Equipment must not be used for personal reasons, including access to the internet.
- Photographs of children must only be taken on school owned property. Staff must never take photographs or record images on personal cameras or equipment (including mobile phones).

- USB devices provided by the school must not be used to store or transfer personal data or electronic photographs.
- Where possible, data should be e-mailed from home rather than transferred on a USB device, especially if it is information downloaded from the internet, so that it undergoes anti-virus scanning.
- Personal devices such as USB devices, mobile phones etc. must never be used to transfer information from home into school to avoid transferring viruses.
- Pupil's personal details, such as full name or addresses, along with photographs of children must not be e-mailed home from school.

For safeguarding issues:

- Mobile phones and other portable technologies owned by staff should be stored in a secure area if brought into school i.e. locked cupboard or locker.
- Equipment such as mobile phones should be turned off during the school day, and should only be used in designated areas; **staff room, office and headteacher's office only.**
- **Some visitors to school, such as SIP, Social Workers or other professionals, may need to receive or make business calls during the course of their visit. This should be done in one of the designated areas above OR in the Conference and Community rooms so long as no children are present.**
- Never share any personal information such as telephone numbers with children.
- Personal mobile telephones should not be used on educational visits. School mobiles should be used in the case of an emergency.
- Never take a child's mobile number or the number of their parents.
- A mobile phone should not be used to record or photograph children for any purpose.

(See also Guidance on Safeguarding for Adults working in School)

Wilful Damage

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.