Samuel Laycock

Happiness First
All Else Follows

E-safety Policy

Policy written:	**January 2016**
Staff Responsible:	**Wendy Charkewycz – ICT Co-ordinator**
Presented to Staff:	**16/11/16**
Review Date:	**12 months from Governor approval (or sooner subject to statutory requirements)**

ICT in the 21st Century is seen as an essential resource to support independent learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Samuel Laycock School needs to develop the use of these technologies in order to arm our students with the skills to access life-long learning and employment. Although ICT is exciting and beneficial both in and out of the context of education, we must recognise that 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 Samuel Laycock School, we understand the responsibility to educate our students on E-safety issues; teaching them the appropriate behaviours and 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.

The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available. The use of email, mobile phones, Internet messaging and blogs all enable improved communication and facilitate the sharing of data and resources. Virtual Learning Environments (VLEs) provide children and/or young adults with a platform for personalised and independent learning.

However, the publicity that surrounds such incidents as children meeting strangers who are older than they have portrayed themselves to be, or Internet scams designed to trick the unwitting email recipient into handing over important bank information are but examples of such negative press reports which raise our awareness of the potential dangers to our young people.

It is important that such views are balanced against the positive benefits technology can bring as a tool to education and also the wider community.
Benefits include:

- Children and/or young adults are equipped with skills for the future.
- The Internet helps to improve children's and/or young adults' reading and research skills.
- Email, Instant Messaging and Social Networking can, if used wisely, help to foster and develop good social and communication skills.

It is important to note that the positive benefits to our young people far outweigh the risks involved, so long as users are made aware of the issues and concerns and receive on-going education in choosing and adopting safe practices and behaviours.

Scope of this document

The scope of the policy is such that it is written in accordance with the former BECTA guidelines; the policy refers to individual technologies currently in school and is subject to review and amendment as new innovations become available to users within the educational framework of Samuel Laycock School.

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-safety of individuals and groups within the school.

Governors
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Head teacher
The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community.

E-Safety Coordinator (currently, Mrs Charkewycz)
The E-safety Coordinator:

- Leads cross-school initiative on E-safety.
- Takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

ICT managed Service Provider
The Managed Service Provider is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the e-safety technical requirements outlined in the school's Acceptable Use Policies and any relevant Local Authority E-Safety Policy and guidance.
- Users may only access the school's networks through a properly enforced password protection policy.

Teaching and Support Staff
Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the E-safety Coordinator.
- They should be aware of the potential for serious child Protection issues to arise from:
    - sharing of personal data
    - access to illegal/inappropriate materials
    - inappropriate on-line contact with adults/strangers
    - potential or actual incidents of grooming
    - cyber-bullying

Parents/Carers

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy
- Accessing the school ICT systems or Learning Platform in accordance with the school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems or Learning Platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

E-Safety Education and Training

Pupils

E-Safety education will be provided in the following ways:
A planned e-safety programme will be provided as part of ICT/PHSE/other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school.
Key e-safety messages will be reinforced as part of assemblies and tutorial/pastoral activities.
Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
A planned programme of formal e-safety training will be made available to staff. It is expected that some staff will identify e-safety as a training need within the performance management process.
All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies

Use of ICT Technologies

Messaging, Chat and Social Networking

These methods of communication and social interaction are now widely accepted in society and naturally our pupils are keen to make use of them. It is envisaged that we will seek to educate our pupils and provide them with a safe environment for such technologies, using LA or nationally agreed and endorsed packages. Until such measures to prepare our pupils are in place the following will continue to apply:

- The use of Instant Messaging (e.g. MSN messenger) is not permitted.
- Use of Social Networking websites, such as Bebo, Twitter, MySpace, Facebook, Habbo, and Piczo is not currently permitted.
- Pupils and staff must not access public or unregulated Chat Rooms.

Cameras and video Recording

Both photography and video recording are a valuable means of capturing evidence of pupil achievement and significant events in school life. However, it is important to understand that this form of media can be misused or raise child protection issues. Therefore, please ensure the procedure outlined in the relevant AUP is followed:

- Any images or videos of pupils must be used appropriately, stored securely on the school network and deleted from cameras or mobile devices as soon as possible.

- Prior parental consent must have been obtained before such images are taken, (consent form signed).

School Website

The school website has an important role in the promotion of the school. It also informs parents, pupils and staff of the events and achievements of the school. It can also be regarded as an important means of communication of information. However, the school website can be viewed by anyone, anywhere in the world and therefore:

- The school should have a designated member of staff who is responsible for approving all content and images to be uploaded onto its website prior to it being published.
- The school website should be subject to frequent checks by the Head teacher to ensure that no material has been inadvertently posted, which might put children / young people or staff at risk.
- Copyright and intellectual property rights must be respected.

Mobile Phones and devices

The school allows staff to bring in personal mobile phones and devices for their own use. However, staff should not contact a pupil or parent/carer using their personal device.

The school would prefer pupils not to bring personal mobile devices/phones to school. If a pupil chooses to bring a mobile device to school it must be handed to a member of staff during Tutorial time, for safe keeping during the day. At all times the device must be switched off.

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

Both staff and pupils bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Wireless games Consoles

These devices may be used as part of a reward by an appropriate member of staff. It is not permissible to use them online or via chat facilities. The school accepts no responsibility for loss or damage, the owner brings them in at his or her own risk.

The following table summarises school policy on ICT devices and electronic communication

	Staff			Pupils		
Communication method or device	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓			✓		
Use of mobile phones in lessons			✓			✓
Use of mobile phones in social time	✓					✓
Taking photos on personal mobile phones or other camera devices			✓			✓
Use of personal hand held devices eg PDAs, PSPs		✓			✓	
Use of personal email addresses in school, or on school network		✓			✓	
Use of school email for personal emails			✓			✓
Use of chat rooms / facilities			✓			✓
Use of instant messaging			✓			✓
Use of social networking sites			✓			✓
Use of blogs			✓			✓
Use of online shopping or auction sites		✓				✓
Use of video broadcasting sites	✓				✓	
Use of the Internet for personal use/entertainment		✓			✓	

CURRENT LEGISLATION

Acts relating to monitoring of staff email

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)
(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to E-safety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of “Children & Families: Safer from Sexual Crime” document as part of their child protection packs.
For more information:
www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an

offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- Access to computer files or software without permission (for example using another person's password to access files)
- Unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- Impair the operation of a computer or program

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Useful Organisations/Weblinks

www.ceop.gov.uk

www.thinkuknow.co.uk

www.internetsafetyzone.co.uk

www.nch.org.uk

www.nspcc.org.uk/helpandadvice

www.childline.org.uk

www.bbc.co.uk/chatguide

www.childnet-int.org/blogsafety/teachers.html

www.nextgenerationlearning.org.uk/safeguarding

www.teachtoday.eu/

www.boltonsafeguardingchildren.org.uk

www.getnetwise.org

http://kids.getnetwise.org/safetyguide/technology/facebook/facebookprivate-audio (Facebook privacy settings guidance)

www.facebook.com/clickceop

http://www.connectsafely.org/

www.connectsafely.org/fbparents

http://www.connectsafely.org/Safety-Advice-Articles/facebook-privacychart-for-teens.html

http://www.education.gov.uk/schools/pupilsupport/behaviour/bullying/cyber/a0010037/cyberbullying-checklist