Samuel Pepys School

ICT Acceptable Use and eSafety Policy

Links with legislation:

Status: Statutory	Drafted by: L Craigen	Date approved: 31/01/2017	By: Gov sub committee P & C
To be reviewed by (Date):	To be reviewed by (SLT/Gov):	Date shared with staff:	To publish on web: Y/N
Adopted as an EPM model:			

Samuel Pepys School
ICT Acceptable Use and eSafety Policy

Contents

- **Introduction**
- **Monitoring of Internet Activity**
- **eSafety**
- **Staff Professional Responsibilities when using ICT**
- **Internet Access**
- **Passwords and Password Security**
- **Appropriate Storage of Images**
- **Acceptable Use of School ICT Equipment including Portable & Mobile ICT**
- **Reviewing this Policy**

Appendices:
Form 1: Acceptable use of ICT agreement for pupils
Form 2: Acceptable use of ICT agreement for staff
Form 3: School Insurance Cover for School Owned Portable Equipment
Form 4: Indemnity Form for personal portable devices to be used in school (pupils)

Introduction

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

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook, Twitter, SnapChat and Instagram
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Podcasting
- Video Broadcasting
- Music Downloading

At Samuel Pepys School we understand the responsibility to educate our pupils on eSafety issues in collaboration with parents and carers; teaching them the appropriate behaviours to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is applicable for all staff, governors, visitors and pupils. It includes equipment which may be provided by the school (such as PCs, laptops, tablets, mobile phones, webcams, whiteboards, digital video equipment, etc); and equipment owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and portable media players, etc). Everybody in the school has a shared responsibility to secure any sensitive information used in their day-to-day professional duties.

This Acceptable Use Policy sits alongside the Safer Working Practice guidance (October 2015) which has been adopted by Samuel Pepys School.

Monitoring of Internet Activity

All internet activity is traceable and logged by the school's internet provider.

Breaches

A breach or suspected breach of policy by a member of staff, either paid or non-paid, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the school disciplinary policy and procedure.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Head or Deputy Head. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Head or Deputy Head or take advice from the Network Manager.

eSafety

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Emma Cortiel. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Cambs LA, CEOP (Child Exploitation and Online Protection) and Childnet. eSafety guidance to be given to staff on a regular and meaningful basis,

Senior Leadership and governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety and positive behaviour including anti-bullying policy and PSHE

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, we have an agreed eSafety scheme of work.

- The school has a framework for teaching e-safety skills
- Educating pupils on the potential dangers of the internet and possibilities these may entail outside of school is embedded in the e-safety curriculum and informally when opportunities arise
- Where appropriate pupils are made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Because of the complexity of their learning needs, pupils are appropriately supported so that they develop an awareness of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff

member. Some pupils will be aware that they can contact an organisation such as '*Childline'* or use the CEOP report abuse button.

eSafety Skills Development for Staff

 Our staff receive information and training on eSafety and how they can promote the 'Stay Safe' online messages in the form of training sessions and staff meetings and through induction and safeguarding training

 New staff receive information on the school's acceptable use policy as part of their induction (Safer Working Practice)

 All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know to contact in the event of any misuse

 All staff are encouraged to incorporate eSafety rules and awareness within their curriculum areas

Managing the School eSafety Messages

 We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used

 eSafety posters will be prominently displayed and developed with pupils as part of the eSafety curriculum

 eSafety advice will be promoted widely through school displays, newsletters, class activities.

Family Involvement in eSafety

We believe that it is essential for parents/carers and families to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies together with the associated risks.

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

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

 The school disseminates information to parents relating to eSafety where appropriate in the form of information sessions, website and newsletter items

Staff Professional Responsibilities when using ICT

Computer Viruses / Malware

 All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick, must be checked for any viruses using school provided anti-virus software before being used

 Never interfere with any anti-virus software installed on school ICT equipment that you use.

 Ensure you connect regularly to the school network to ensure regular anti-virus updates.

 If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact ICT Network Manager or Deputy Head immediately.

Staff Email Accounts

 The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff and avoids the risk of personal profile information being revealed

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

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

 E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Receiving Emails

 Check your e-mail regularly

 Never open attachments or click on links in an email from an untrusted source, by wary of an unexpected / unusual email from a purported known souce; Consult the network manager first

 Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

 The automatic forwarding and deletion of e-mails is not allowed

Pupil Email Accounts

 In line with their course of study, pupils, most likely in KS4 and Post 16, they will only use a school approved email account

 All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

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

 All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

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

 Staff must inform the Head/Deputy if they receive an offensive e-mail

 Pupils are introduced to e-mail as part of their course of study

 Pupil school email accounts will only be used throughout the course of the school day and linked to an approved course of study.

Internet Access

The internet is an open worldwide communication medium, available to everyone at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

 The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity

 Staff will preview any recommended sites before use

 Raw image searches are discouraged when working with pupils

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

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

 All users must observe copyright of materials from electronic resources

Staff Use of the Internet

 Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

 Staff may use the school name or school email address to access approved websites in consultation with SLT

 Do not reveal names of the school, colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application

 On-line gambling or gaming is not allowed

Management of ICT Infrastucture

 School internet access is controlled through the LA's web filtering service, Cambridgeshire ICT Service

 Staff and pupils are aware that school based email and internet activity can be monitored and is traceable

 If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or Deputy Head as appropriate

 It is the responsibility of the school, by delegation to the Network Manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines. Staff are reminded that sensible usage behaviour is more important than having anti virus, which even when up to date may not protect against recent threats

 Pupils and 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 and to consider the use of encryption (e.g. BitLocker to go) especially if sensitive information is stored. It is not the school's responsibility nor the Network Manager's to install or maintain virus protection on personal systems

 Use of personal accounts on 'cloud' storage services, such as dropbox, onedrive etc are only permitted with SLT consent

 If there are any issues related to viruses or anti-virus software, contact Network Manager

Passwords and Password Security

Passwords

 Always use your own personal passwords

 Staff should change temporary passwords at first logon

 Change passwords whenever there is any indication of possible system or password compromise

 Do not record passwords or encryption keys on paper or in an unprotected file

 Only disclose your personal password to authorised ICT support staff in person when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

 Never tell a child or colleague your password

 If you are aware of a breach of security with your password or account inform the Network Manager immediately

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Pupil passwords will be kept private/secure with class teacher and should not be shared with other users. Staff and pupils are regularly reminded of the need for password security.

- Some of our pupils may be able to access programs and emails independently, therefore we have a 'Pupil' login account for all pupils which has appropriate restrictions in place.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked
- Due consideration should be given when logging into the school network, virtual learning environment or other online application to the browser/cache options (shared or private computer)
- Pupil passwords for educational resources such as Education City are retained by the class teacher and e-Safety Co-ordinator.

Appropriate Storage of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

 With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

 Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils without advance permission from the Headteacher. This includes when on field trips. School provides portable devices for taking images.

 Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher

 Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

Publishing Pupil's Images and Work

On a child's entry to the school and via the annually updated Essential Information Form, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

 on the school web site

 in the school prospectus and other printed publications that the school may produce for promotional purposes

 recorded/ transmitted on a video or webcam

 general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically) This consent is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by parents/carers in order for it to be deemed valid.

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

Before posting pupil work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. (see Essential Information Form in main office)

Storage of Images

 Images/ films of pupils are stored on the school's computer equipment and network only

 Images of pupils and staff are not permitted to be stored indefinitely on portable media for (e.g., USB sticks)

 Rights of access to these images are restricted to the staff and pupils within the confines of the school network or other online school resource

 At the end of each school year the class teacher has the responsibility to retain a small number of images of each of the pupils in their class and saved in the relevant pupil file, demonstrating a particular skill or achievement and deleting all others.

Acceptable Use of School ICT Equipment including Portable & Mobile ICT

School ICT Equipment

 All adult users of the school ICT equipment are responsible for their activity and the pupils in their care

 The Network Manager logs ICT equipment issued to staff and pupils and records serial numbers as part of the school's inventory

 Visitors are not permitted to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities available

 All ICT equipment is kept physically secure
 Unauthorised modifications to computer equipment, programs, files or data is not permitted. This is an offence under the Computer Misuse Act 1990
 Data is saved on a frequent basis to the school network. Individuals are responsible for the backup and restoration of any of the data that is not held on the school's network
 Personal or sensitive data should not be stored indefinitely on the local drives of desktop PC, laptop, USB memory stick, or other portable device.
 Privately owned ICT equipment is not permitted to be used on a school network, without the headteacher and ICT managers approval.
 On termination of employment, resignation or transfer, all ICT equipment should be returned to the Deputy Head.
 It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
All ICT equipment allocated to staff is authorised by the Deputy Head responsible for:
 maintaining control of the allocation
 recovering and returning equipment when no longer needed
 all redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment
This section covers such items as laptops, mobile devices and removable data storage devices.
 All activities carried out on school systems and hardware will be monitored in accordance with the general policy
 Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
 Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey. Laptops should never be left in a car.
 Synchronise all locally stored data, with the central school network server on a frequent basis
 Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
 The installation of any applications or software packages must be authorised by the ICT Manager, fully licensed and only carried out by the ICT Manager
 In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
 Portable equipment must be transported in its protective case if supplied

Personal Mobile Devices for staff (including phones)
 The school allows staff to bring in personal mobile phones and devices for their own use, outside of directed time, unless agreed otherwise for exceptional circumstances. Only under exceptional circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
 The school is not responsible for the loss, damage or theft of any personal mobile device
 The sending of inappropriate messages or emails between any member of the school community is not allowed
 Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including iPads and mobile phones)
 No inappropriate apps to be downloaded onto iPads, staff need to be vigilant at checking the suitability of apps before downloading
 The sending of inappropriate messages or emails between any member of the school community is not allowed

 Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
 When using a school mobile phone, you are responsible for the security of the phone. Do not leave it unattended and on display (especially in vehicles)
 Report the loss or theft of any school mobile phone equipment immediately
 The school remains responsible for all call costs until the phone is reported lost or stolen
 You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it
 School SIM cards must only be used in school provided mobile phones
 Refrain from calling premium rate numbers and any numbers outside of the UK
 Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so

Personally Provided Mobile Devices for use by Pupils (including iPads and phones)
Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. Pupils and their families remain responsible for these devices whilst in school. At all times during the school device must be switched off or on silent
 Pupils may bring a personal mobile device into school where specifically agreed as a communication device, in line with speech and language therapy advice. Please see Appendix Four for an indemnity form.

Social Media
Facebook and other forms of social media are increasingly becoming an important part of our daily lives.
 Staff ***should not*** access their personal social media accounts using school equipment
 Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
 Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
 Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Reviewing this Policy
There will be on-going opportunities for staff to discuss with the eSafety coordinator any esafety issue that concerns them. This policy will be reviewed regularly and consideration given to the implications for future whole school development planning
The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Appendix One
Samuel Pepys School Acceptable Use Agreement: Pupils

These are our eSafety Rules. I agree…

☑ I will only use ICT in school for school purposes.
☑ I will only use ICT in school when a member of staff is present.
☑ I will only use my own school email address when emailing as part of course of study.
☑ I will only open email attachments from people I know
☑ I will not tell other people my ICT passwords. (Unless I am asked to share to keep me safe)
☑ I will only open/delete my own files.
☑ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
☑ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
☑ I will not give out my own details such as my name, phone number or home address.
☑ I will not use my own device to take photos or videos or other pupils or staff or share these on social media.
☑ I will not use the schools name (Samuel Pepys School) in social media unless specifically requested to do so, for example to share a fundraising request.
☑ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
☑ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.
Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the class teacher or our eSafety Co-ordinator

We have discussed this and my son/daughter agrees to follow the eSafety rules and to support the safe use of ICT at Samuel Pepys School.

Pupil Name:	Signature:	
Parent/ Carer Name:	Signature:	Date

Appendix Two
Samuel Pepys School Acceptable Use Agreement for Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the ICT coordinator or the headteacher.

☑ I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
☑ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
☑ I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
☑ I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
☑ I will only use the approved, secure e-mail system(s) for any school business.
☑ I will ensure that personal data (such as data held on SPS systems) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body
☑ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
☑ Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
☑ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
☑ I will not use the schools name (Samuel Pepys School) in social media unless specifically requested to do so, for example to share a fundraising request.
☑ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
☑ I will respect copyright and intellectual property rights.
☑ I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute in line with Safer Working Practice.
☑ I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
☑ I understand this forms part of the terms and conditions set out in my contract of employment.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout Samuel Pepys School

Full Name:	Signature:	Date:

Appendix 3: School Insurance Cover for School Owned Portable Equipment

School Insurance Cover for School Owned Portable Equipment

Item name/description _____

School owned portable equipment e.g. Laptops and iPads are insured off site and whilst in a teachers home.

However, if they are left in an unattended vehicle they must be stored out of sight.

They are NOT insured if left in a vehicle overnight.

I confirm that I have read and understood the instructions for keeping School Owned Portable Equipment secure and that this a requirement of the Cambridgeshire County Council insurance policy which Samuel Pepys School buys into.

Signed: _____

Print Name: _____ Date: _____

Appendix 4: Indemnity Form: For personal portable devices approved for use in school (pupils)

Indemnity Form

For personal portable devices approved for use in school (pupils)

Personal portable devices include items such as Laptops / Tablets / Communication aids.

Item name/description: _____

Samuel Pepys insurance would cover loss or damage to school approved personal computer equipment owned by _____ where the loss, damage or injury arises as result of the negligence of the school (e.g. if it was stolen from the school premises).

However if a pupil was to drop or damage the device this would not be covered by the school insurance. Although this may be covered by your household insurance.

We confirm that in the event of the device being damaged by another pupil, either accidentally or in the unlikely event of intentional damage we would repair or replace it on the first occasion and review its use in school.

The device will be housed in a protective case at all times.

Signed: _____ Date: _____

Headteacher

_____ Date: _____

Class Teacher

_____ Date: _____

Parent