Stanbridge Primary School

ICT

(Including E-Safety and Acceptable Use)

POLICY

Signed (Chair):	Name: Mrs M Todd	Date: 19/06/17
Signed (Headteacher):	Name: F Bertham	Date: 19/06/17
Ratified: by Curriculum Committee	Next Review: Term 6 (17/18)	

Equality Impact Assessment (EIA) Part 1: EIA Screening

Policies, Procedures or Practices	ICT inc E-Safety & Acceptable Use Policy	**Date:**	9th May 2016
EIA CARRIED OUT BY:	F Bertham	EIA APPROVED BY:	F Bertham

Groups that may be affected:

Are there concerns that the policy could have a different impact on any of the following groups? *(Please tick the relevant boxes)*	**Existing or potential adverse impact**	**Existing or potential for a positive impact**
Age (young people, the elderly; issues surrounding protection and welfare, recruitment, training, pay, promotion)		
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication)		
Gender Reassignment (transgender)		
Marriage and civil partnership		
Pregnancy and maternity		
Racial Groups (consider: language, culture, ethnicity including gypsy/traveller groups and asylum seekers)		
Religion or belief (practices of worship, religious or cultural observance, including non-belief)		
Gender (male, female)		
Sexual orientation (gay, lesbian, bisexual; actual or perceived)		

Any adverse impacts are explored in a Full Impact Assessment.

Stanbridge Primary School

ICT Policy (Incl. E-Safety & Acceptable Use

This e-safety policy has been developed, and will be reviewed and monitored annually, by our school e-safety working group which comprises:

- School E-Safety Co-ordinator
- ICT Subject Leader
- Headteacher
- A representative of teaching staff
- A Governor representative and a parent representative

Consultation with the whole school community has taken place through a staff meeting, Student Council meeting, Governors' meeting, parents' evening and the school website/newsletter.

Schedule for Development, Monitoring and Review

This e-safety policy was approved by the Governors' Curriculum & Monitoring Committee on: 19th June 2016	
The implementation of this policy will be monitored by the	e-safety working group
Monitoring will take place at regular intervals	annually during Term 6
The Curriculum & Monitoring Committee will receive a report on the implementation of this policy including reported incidents	annually during Term 6
This policy will be reviewed regularly and in the light of significant new developments or threats to e-safety	annually during Term 1
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Integra: HR for Schools – Safeguarding Schools' IT, Dylan Burnell – Technical Schools' IT, Jo Briscombe – ICT Strategy Adviser

The school will monitor the impact of the policy using:

- logs of reported incidents
- SWGfL (South West Grid for Learning) monitoring logs of internet activity and any network monitoring data from the LA technical team
- questionnaires/surveys of pupils, parents/carers and staff including non-teaching staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, in school and also out of school where actions relate directly to school-set activity or use of school online systems. The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents (such as cyber-bullying) which may take place out of school but are linked to membership of the school. The school will deal with such incidents according to this policy and associated behaviour and anti-bullying policies and will inform parents/carers of known incidents of inappropriate e-safety behaviour that take place out of school.

It is the school's responsibility to ensure children are safe from terrorist and extremist material when accessing the internet in school. The school will ensure that suitable filtering is in place and will play an important role in equipping children and young people to stay safe online, both in school and outside.

The following sections outline the roles and responsibilities, policy statements and education relating to e-safety for individuals and groups within the school.

Roles and Responsibilities

These are clearly detailed in Appendix 1 for all members of the school community.

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator.
The designated person for child protection is trained in e-safety issues and is aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults/strangers, or potential or actual incidents of grooming and cyber-bullying.

Staff and Governors

There is a planned programme of e-safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this and the acceptable use policies.

- An audit of the e-safety training needs of all staff is carried out annually.
- All new staff receive e-safety training as part of their induction programme.
- The E-Safety Co-ordinator receives regular updates through attendance at LA training sessions and by reviewing regular e-safety updates from the local authority.
- This e-safety policy and its updates are shared and discussed in staff meetings.
- The E-Safety Co-ordinator provides advice/guidance and training to individuals and seeks LA advice on issues where required.

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of pupils in e-safety is therefore an essential part of our school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

- There is a planned e-safety programme (scheme of work) detailed below.
- Key e-safety messages are reinforced annually through an assembly.
- Pupils are helped to understand the pupils' acceptable use policy and act accordingly.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems are posted in all rooms where ICT is used and also displayed on log-on screens.
- Staff act as good role models in their own use of ICT.

Curriculum

E-safety is a focus in all relevant areas of the curriculum. The e-safety scheme of work follows Common Sense Media. For each year group it identifies progression statements, learning outcomes, processes, skills and techniques, vocabulary, suggested software and web links, sample activities and assessment activities.

- In lessons where internet use is planned, pupils are guided to sites checked as suitable for their use, and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to search the internet freely, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit, and encourage students to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Pupils are taught to be critically aware of the materials and content they access on-line and to assess the accuracy of information (including 'fake news').
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will use and apply SMART rules when online. **S** (Keep **safe** by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password). **M** (**Meeting** someone you have only been in touch with online can be dangerous. Only do so with your parents or carers permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time). **A** (**Accepting** emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems they may contain viruses or nasty messages!). **R** (Someone online might lie about who they are and information on the internet may not be true or **reliable**. Always check information with other websites, books or someone who knows. If you like chatting online it's best to only chat to your real world friends and family). **T** (**Tell** your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online).

Parents / Carers

Parents and carers may have only a limited understanding of e-safety issues and may be unaware of risks and what to do about them, they have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents to do this by:

- providing clear Acceptable Use Policy guidance, newsletter and web site updates
- providing an awareness-raising meeting for parents
- inviting parents to attend activities such as e-safety assemblies

Technical Staff - Roles and Responsibilities

Technical support is provided by South Glos Technical Support team (01454 863838).
For all schools, the local authority provides technical guidance for e-safety issues, and the team is fully informed about the issues. Where the local authority provides technical support the "administrator" passwords for the school are not held by the school and the local authority is responsible for their security and any implications of their use.
The school ensures, when working with our technical support provider, that the following guidelines are adhered to:

- School ICT systems are managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Use Policy and relevant Local Authority e-safety guidance.
- There are regular reviews of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems.
- All users are provided with a username and password by the technical support provider.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any evidence or suspicion that there has been a breach of security.
- The school upholds and supports the managed filtering service provided by SWGfL.
- In the event of the school technician needing to make requested changes to filtering, or for any user, this is logged and carried out by a process that is agreed by the Headteacher.

- Any filtering issues are reported immediately to the South Gloucestershire technical team.
- School ICT technical staff regularly monitor and record the activity of users on the school's ICT systems and users are made aware of this in the Acceptable Use Policy.
- Actual and potential e-safety incidents are documented and reported immediately to the E-safety Leader who will arrange for these to be dealt with immediately in accordance with the acceptable use policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc. from accidental or malicious attempts which might threaten the security of the school's systems and data.
- The provision of temporary access for "guests" (e.g. trainee teachers, visitors, supply teachers) to the school system must be approved and completed by the technical support provider.
- Teaching and administrative staff only are allowed to download executable files and these must be for educational purposes.
- Teaching and administrative staff are allowed to use laptops and other portable devices assigned to them out of school for personal use. The laptops and other portable devices are for their sole personal use only and should be used in accordance with the guidelines set out in this policy and other related policies. Laptops and other portable devices assigned to pupils can be used out of school for educational use only (see the Data Protection section for further detail).
- Teaching and administrative staff only can request programmes to be installed on school workstations/portable devices but this must be approved and completed by the technical support provider.
- Teaching and administrative staff only are allowed the use of removable media (e.g. memory sticks/CDs/DVDs) on school workstations/portable devices. These must be provided by the school and are for educational use only.
- The school infrastructure and individual workstations are protected by up to date virus software.
- The school infrastructure and individual workstation software are updated by the school technical support provider.
- The school infrastructure and individual workstation security updates/patches for the operating system are kept up to date by the school technical support provider.
- Personal data may not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are reported incidents of employers carrying out internet searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm.

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but follow guidance in the Acceptable Use Policy concerning the sharing, distribution and publication of those images.
- Staff ensure that pupils also act in accordance with their Acceptable Use Policy.
- Pupils' work is only published on a public web site with the permission of the pupil and parents or carers.

Data Protection

Staff must ensure that they:

- take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- use personal data only on secure password-protected computers and other devices, ensuring that they are properly logged off at the end of any session in which they are using personal data
- restrict the storage of school-related personal data to school equipment (including computers and portable storage media)
- transfer data using encryption and secure password-protected devices

When personal data are stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password-protected
- the device must be protected by a password plus virus and malware checking software (many memory sticks/cards and other mobile devices cannot be password protected and therefore should not be used)
- the data must be securely deleted from the device once it has been transferred or its use is complete

Guidance on the Use of Communications Technologies

A wide range of communications technologies have the potential to enhance learning.

- The official school email service is used for communications between staff and with parents/carers and pupils as it provides an effective audit trail.
- Any digital communication between staff and pupils or parents/carers (email, chat, VLE etc.) must be professional in tone and content. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications. Pupils' names will not be used in full (initials only) for staff email communication.
- Users are made aware that email communications may be monitored and are informed through the Acceptable Use Policies of what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use only.
- Pupils are taught about email safety issues through the scheme of work and implementation of the Acceptable Use Policy.
- Personal information is not sent via e-mail as this is not secure. Personal information is also not posted on the school website and only official email addresses are listed for members of staff.

The following table shows how the school currently considers these should be used.

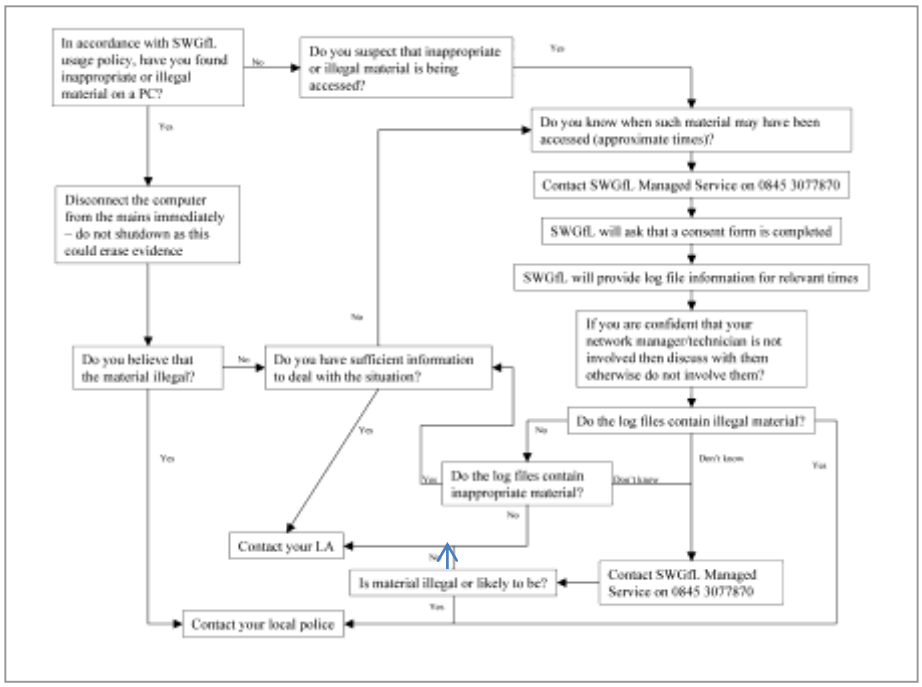
	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√						√	
Use of mobile phones in lessons				√				√
Use of mobile phones in social time	√							√
Taking photos on mobile phones	√*							√
Taking photos on other camera devices	√						√	
Use of hand held devices e.g. 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	√							√

√* **Deleted once copied onto system**

Responding to incidents of misuse

We expect all members of the school community to be responsible users of ICT who understand and follow this policy. However, there may be times when infringements of the policy occur through careless, irresponsible or, very rarely, deliberate misuse. If any apparent or actual misuse appears to involve illegal activity the SWGfL flow chart below is consulted and followed, in particular the sections on reporting the incident to the police and the preservation of evidence. Illegal activity would include:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials



If members of staff suspect that any misuse might have taken place it is essential that correct procedures be used to investigate, preserve evidence and protect those carrying out the investigation. In such an event the SWGfL “Procedure for Reviewing Internet Sites for Suspected Harassment and Distress” will be followed. This guidance recommends that more than one member of staff be involved in the investigation which should be carried out on a “clean” designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents be dealt with as soon as possible in a proportionate manner, and that members of the school community be made aware that incidents have been dealt with.

Unsuitable / inappropriate activities

The school believes that the activities referred to below are inappropriate in a school context and that users should not engage in these activities in school, or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					√
	the promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation					√
	adult material that potentially breaches the Obscene Publications Act in the UK					√
	criminally racist material in the UK					√
	pornography				√	
	the promotion of any kind of discrimination				√	
	the promotion of racial or religious hatred				√	
	threatening behaviour, including promotion of physical violence or mental harm				√	
	any other information which may be offensive to colleagues, breaches the integrity of the ethos of the school or brings the school into disrepute				√	
using school systems to run a private business					√	
using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and/or the school					√	
uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					√	
revealing or publicising confidential or proprietary information (e.g. financial/ personal, databases, computer/network access codes and passwords)					√	
creating or propagating computer viruses or other harmful files					√	
carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet					√	
on-line gaming (educational)			√			
on-line gaming (non-educational)					√	
on-line gambling					√	
on-line shopping/commerce				√		
file sharing				√		
using social networking sites e.g. Bebo, Facebook for older users				√		
using video broadcasting e.g. Youtube				√		

Appendix 1

Roles and Responsibilities

Role	Responsibility
Governors	• Approve and review the effectiveness of the E-Safety Policy and acceptable use policies • E-Safety Governor works with the E-Safety co-ordinator to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering, and then reports to Governors
Head teacher and Senior Leaders	• Ensure that all staff receive suitable CPD to carry out their e-safety roles and that sufficient resources are allocated • Ensure that there is a system in place for monitoring e-safety • Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff • Inform the local authority of any serious e-safety issues including filtering • Ensure that the school infrastructure/network is safe and secure and that policies and procedures approved within this policy are implemented
E-Safety Co-ordinator	• Lead the e-safety working group and deal with day to day e-safety issues • Take a leading role in establishing/reviewing e-safety policies/documents • Ensure all staff are aware of the procedures outlined in policies • Provide and/or broker training and advice for staff • Attend updates and liaise with the LA e-safety staff and technical staff • Deal with and log e-safety incidents • Meet with E-Safety Governor regularly to discuss incidents and review the log • Report regularly to Senior Leadership Team
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Have read, understood and signed the Staff Acceptable Use Agreement (AUP) • Act in accordance with the AUP and E-Safety Policy • Report any suspected misuse or problem to the E-Safety Co-ordinator • Monitor ICT activity in lessons, extracurricular and extended school activities
Pupils	• Participate in e-safety activities, follow the Acceptable Use Policy and report any suspected misuse • Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school
Parents and carers	• Endorse (by signature) the Pupil Acceptable Use Policy • Ensure that their child/children follow acceptable use rules at home • Discuss e-safety issues with their child/children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet • Access the school website/Merlin in accordance with the relevant school Acceptable Use Policy • Keep up to date with issues through school updates and attendance at events
Technical Support Provider	• Ensure the school's ICT infrastructure is secure in accordance with South Gloucestershire guidelines and is not open to misuse or malicious attack

	• Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data • Inform the Headteacher of issues relating to filtering • Keep up to date with e-safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator for investigation/action/sanction. • Ensure monitoring software/systems are implemented and updated • Ensure all security updates/patches are applied (including up to date anti-virus definitions, Windows updates) and that reasonable attempts are made to prevent spyware and malware.
Community Users	• Sign and follow the AUP before being provided with access to school systems.

Acceptable Use Policy
Introduction

Introduction:

1. The Acceptable Use Policy (AUP) is broken down into several specific policies which define the rights and responsibilities of the following groups:
    i. Parents/Carers
    ii. Staff and Volunteers
    iii. KS1 Pupils
    iv. KS2 Pupils

2. These policies define acceptable practice by each group, and individuals are expected to sign and return the appropriate form to demonstrate that they understand and agree with the policy.

3. **Parents/Carers** will only need to sign the policy once, usually when their child enters the school.

4. **Staff and Regular Volunteers** will be asked to sign the policy as part of their induction.

5. **Supply Teachers** will be asked to familiarise themselves with the policy which will be available in the class supply pack.

6. **Occasional Volunteers** are not given access to school IT resources, so will only be asked to sign the policy if their work involves the use of technology.

7. Breaches of this policy will be dealt with in accordance with the E-safety Policy and staff disciplinary policy where appropriate.

Stanbridge Primary School
Rules for Keeping Safe with ICT

Key Stage 1

- I will ask a teacher when I want to use the computer or contact people using ICT.
- I will use a computer only when an adult is present.
- I will use only the web sites that I am allowed to.
- I will keep my password secret and not tell it to anyone.
- I will be polite and friendly when I use the computer to contact people.
- I will keep my personal details secret and not tell anybody about my home, family and pets. I will keep my friends' details secret too.
- I know that things I put up on the internet can be seen by anyone and I will not upload anything without asking an adult first.
- I will not take or share pictures of anyone without asking them first.
- I will check information I find online as it might not be true.
- I know that I should not buy anything on line.
- I will tell a teacher (or adult I trust) if I find anything on a computer or a message that is mean, upsetting or worrying.
- I will tell a teacher (or adult I trust) if I know of anyone who is behaving badly on line or if I know anyone may be being bullied.

I will use ICT by these rules when:

- I use school ICT.
- I use my own ICT out of school for school activities.

If I deliberately break these rules then I know that there will be consequences.

My Name is

My Class teacher is

Signed

Date

Stanbridge Primary School
Key Stage 2 - Rules for Keeping Safe with ICT

Content
- I will use clear search words so that I find the right information.
- I know that some content may not be filtered out and what to do if I find something worrying.
- I will double check information I find online.

Contact
- I know that I need to behave well online as in real life and be polite and friendly.
- I will not open messages if the subject field is not polite or if I do not know who they are from.
- I am careful about what I send as messages can be sent on to my parents or headteacher.
- I know that I must have permission to communicate online and will make sure my teacher/ parents know who I communicate with.
- I will talk to an adult if an online friend wants to meet me and will never arrange to meet anyone without permission.
- I know that anything I put up on the internet can be seen by anyone.
- I will only use my mobile phone at school for things that the school allows.

Conduct
- I will not use ICT in school without permission from my teacher.
- I will choose my user names and passwords carefully to protect my identity and I will not share them. I will not ask computers to remember my password.
- I know I must keep my personal details and those of others private.
- I will not visit unsafe sites or register for things I am not old enough for.
- I will log off sites when I have finished.
- I know that I should not buy anything on line without permission.
- I will not use anyone else's work or files without permission.
- Where work is protected by copyright, I will not try to download copies.
- I will not take or share pictures of anyone without their permission.

Problems
- I will not try to change computer settings or install programmes.
- I will not damage equipment and will tell a teacher if equipment is broken or not working.
- I will tell a teacher or adult I trust if I find anything on a computer or a message that is unpleasant or makes me feel uncomfortable.
- I will tell a teacher or adult I trust if I know of anyone who is behaving badly on line or anyone who may be being bullied.

I agree to use ICT by these rules when:
- I use school ICT or my own in school (including my mobile phone when allowed).
- I use my own ICT (including mobile phone) out of school to access school sites or for school activities.

I understand that if I break these rules there could be the following consequences:
(1) I might have a sanction in class e.g. missed playtime etc.
(2) I might not be allowed to use the internet or other applications in school.
(3) I might be sent to Miss Bertham and my parents called into school.
(4) I could be excluded if I damage things, share inappropriate material, cyber-bully or break the law.

My Name is	
My Class teacher is	

Signed _____ Date _____

Stanbridge Primary School

Staff Acceptable Use Policy

Policy Context

Technologies and the internet, including social media, are powerful tools which open up new opportunities for learning and teaching. They can motivate learners, promote creativity, and support effective learning, assessment and engagement with parents. They also bring opportunities to enhance teaching, increase staff efficiency and provide opportunities for staff to benefit from professional development through networking and collaboration. All users have an entitlement to good, safe access to ICT and the internet. This Acceptable Use Policy is intended to ensure that:

- staff and volunteers are responsible users and stay safe while using technologies
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- staff are protected from potential risk from the use of ICT in their everyday work, and work to ensure that young people in their care are safe users.

Content

- I know that all school ICT is primarily intended for educational use and I will not use the systems for personal or recreational use during the school day.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not make large downloads or uploads that might take up excessive internet capacity.
- I understand that our school uses only services which mean that my data are stored in the U.K. (e.g. Cloud storage systems) where data includes information about children.
- Staff may use Cloud storage systems (Dropbox, Apple Cloud, etc.) for learning resources which do not make reference to children, but do so at their own risk.

Contact

- I will communicate online in a professional manner and tone and I will not use aggressive or inappropriate language.
- I will only communicate with pupils and parents/carers using official school systems.
- I will not 'friend' parents and/or pupils on social networking sites.
- I am aware that any communication could be forwarded to an employer or Governors.
- I will only use chat and social networking sites for school purposes that are approved by the school.
- I will not use personal email addresses on the school ICT systems without permission.
- I will not open any attachments to emails unless the source is known and trusted, due to the risk of the attachment containing viruses, inappropriate content or other harmful programmes.
- I will use only my own user names and passwords which I will choose carefully so they cannot be guessed easily. I will not use any other person's username and password.
- I will not make contact with parents/pupils via the school Facebook page - the school policy is for Facebook to be used only by children over the age of 13.

Conduct

- I will use school equipment only for the purposes of learning and teaching.

- I will not engage in any online activity that may compromise my professional responsibilities or compromise the reputation of the school or its members. This includes use of the school e-mail account, logo or my school role.
- I will ensure that my data are regularly backed up.
- I will ensure that data kept in Cloud storage do not contain personal data relating to children e.g. addresses, dates of birth, etc.
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when I am required by law or by school policy to disclose them to an appropriate authority.
- I will only transport, hold, disclose or share personal information, about myself or others, as outlined in the school personal data policy. I will not send personal information by e-mail as it is not secure.
- Where personal data are transferred outside the secure school network, they must be encrypted.
- I will not try to bypass the filtering and security systems in place.
- I will only use my personal ICT (including mobile phones, iPads, laptops) in school for learning and teaching activities with permission from the Headteacher or Deputy Head and, if permission is granted, I will follow the rules set out in this agreement.
- My mobile phone will be stored safely and will not be accessed during learning and teaching time (unless permission is granted by HT/DH). During break times/lunchtimes, I will only use my personal device for activities that do not breach the AUP and the E-Safety policies.
- I will only save images/film of children on non-school equipment where there is a specific educational reason which has been sanctioned by the school (agreed by HT and DH). These images will be kept only as long as necessary to complete the agreed task and no images/film of children will be kept on personal devices for extended periods of time.
- When I have used my personal device to record video/images, I will delete the image as soon as I have saved it to, for example, the school website or network.
- I will only take images or video of pupils/staff where it relates to agreed learning activities and will ensure I have parent/staff permission before I take them. If these are to be published online or in the media I will ensure that parental/staff permission allows this.
- Where these images are published (e.g. on the school website, Facebook, etc.) I will ensure it is not possible to identify the people who are featured by name or other personal information.
- I understand my photograph may be used on the school website, which means that it could be copied by others. I know that where it is used my photograph will not be accompanied by any personal details, other than my name.
- When I use my teacher laptop at home I will ensure resources cannot be accessed or copied by anyone else and that no one else uses the laptop.
- I will not install or store programmes on a school device unless I have permission.
- I will not try to alter computer settings, unless this is allowed in school policies.
- I will not cause damage to ICT equipment in school and will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not access, copy, remove or otherwise alter any other users' files without their permission.
- I will ensure that I have permission before using the original work of others in my own work and will credit them if I use it. Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Promoting Safe Use by Learners

- I will model safe use of technologies and the internet in school.
- I will educate young people about how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school policy if an issue arises in school that might compromise pupil, user or school safety or if a child reports any concerns.

- I will monitor pupil behaviour online when using technology and deal with any issues that arise.

Problems

- I will immediately report to the E-safety Co-ordinator or Headteacher any illegal, inappropriate or harmful material or incident I become aware of.
- If I believe a member of staff is infringing this policy, or putting themselves or others at risk, I will report this to the Headteacher.
- **If I believe a young person may be at risk I will follow the child protection procedures.**
- **If I believe a young person may be being bullied I will follow the anti-bullying procedures.**

Sanctions

I understand that breaches of the policy will result in the following sanctions:

- Illegal activities – suspension and report to police (See E-safety Policy).
- Unacceptable activities – Formal Disciplinary Action (See Disciplinary Policy).

(See E-safety Policy Appendix for details)

Staff / Volunteer Name	
Signed	
Date	

Stanbridge Primary School

Parent/Carer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. Technologies open up new learning opportunities for everyone. They can stimulate discussion, promote creativity and effective learning, and promote more effective communications between parents/carers and the school in order to support young people with their learning. Young people should have an entitlement to safe internet access.

This Acceptable Use Policy is intended to ensure that:

- all young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their online behaviour

The school will try to ensure that pupils have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents/ carers will be aware of the school's expectations of the children in their care.

Parents/carers are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Home Use of the Internet

We hope you will reinforce the issues contained in the Pupil Acceptable Use Policy when your child uses the internet at home. In order to do this we recommend that you:

- Ensure that children access the internet in a communal room.
- Ensure supervision appropriate for the age of your child including supervising all use of the internet by younger users.
- Set appropriate rules for using the ICT and the internet safely at home. The school rules could provide a starting point.
- Inform the school if you have concerns which the school could help to address through teaching.
- Ask your child about the sites they are visiting.
- Ensure that family computers are password-protected and have robust anti-virus software which is regularly updated.
- Ensure content is appropriately filtered for younger users; most internet providers have this service available.
- Ensure that your child knows that any protection system does not stop all unsafe content and that they need to tell you if they access something inappropriate or get an upsetting message.
- Reassure your child that if they talk to you about a problem they are having on the internet you will not ban them from using it as this would discourage them from telling you.

- Ensure that your child knows not to leave computers logged on with their user name or logged on to sites with personal details entered, as others could use them.

In order to support those parents who may be less familiar with use of the internet we have listed a variety of additional measures that you could take at home to support your child's safe use of the internet.

Additional Guidance on Safe Use of ICT at Home

Keeping Safe

- Discuss user names with children and talk about how to choose them carefully to protect their identity.
- Talk to young people about the information they should keep private in order to prevent them being contacted or traced including full name, address, telephone number, school, places they go to regularly.
- Talk to young people about the need to limit access to their own information by using the safety and privacy features of sites to give access only to people they know and to be careful who they add as friends.
- Model safe behaviour in your use of ICT.

Research and fun on the internet

- Talk to your child about the fact that any information published on the web can be read by anyone and that they should only publish information they would be happy for anyone to read.
- Check information that younger users are publishing on the web before it is posted to ensure that they are not putting themselves at risk.
- Check that they are old enough for the sites they are using.

Communicating

- Discuss the need for young people to be polite to others online and that they should not use bad language or comments which might upset others.
- Discuss the fact that e-mails/messages can be intercepted and forwarded to anyone (including parents, Headteacher or future employer)!
- Ensure that young people know they should not open messages if the subject field contains anything offensive or if they do not recognise who it is from and that the safest thing to do is to delete it without opening it.
- Recognise that there is a difference between online friends who you will never meet and real world friends. Talk to your child about their online friends.
- Remind your child that people they talk to online may not be who they seem.

Sharing

- Ensure your child knows that downloading games and music that are copyrighted without paying for them is illegal.

Buying and Selling Online

- Help young people to tell the difference between web sites for information and web sites used to sell items.
- Discuss how to recognise commercial uses of the internet e.g. iTunes, mobile phone downloads, shopping.
- Remind young people that if an offer looks too good to be true it probably is and that they should not respond to unsolicited online offers.
- Remind young people that they should not purchase or download anything that costs money without asking permission and that they should not use someone else's identity to buy things online.

Problems

- Ensure that they know that if they receive an offensive or worrying message/e-mail they should not reply but should save it and tell you.

Permission Form

Please complete the information below and return to school.

Parent/Carer Name	
Pupil Name	

As the parent/carer of the above pupil, I give permission for my child to have access to the internet and to ICT systems at school.

I know that my child has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

Signed	Date

Stanbridge Primary School

Volunteer Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety of other staff and pupils or to the security of the ICT systems.

I understand that these rules are in place to enable me to use ICT safely and that if I do not follow them I may be subject to disciplinary action. I agree to use ICT by these rules when:

- I use school ICT systems at school or at home when I have permission to do so
- I use my own ICT (including mobile phone) in school
- I use my own ICT out of school (including mobile phone) to access school sites or for activities relating to my role at the school

I know that the school will monitor my use of the school ICT systems and communications.

Problems

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the E-safety Co-ordinator or Headteacher.
- If I believe a member of staff is infringing this policy, or putting themselves or others at risk, I will report this to the Headteacher.
- **If I believe a young person may be at risk I will follow the child protection procedures.**
- **If I believe a young person may be being bullied I will follow the anti-bullying procedures.**

Use of Staff Images on School Publicity and Web sites

- I understand my photograph may be used on the school web site, which means that it could be copied by others. I know that where it is used my photograph will not be accompanied by any personal details.

Staff / Volunteer Name	
Signed	
Date	

November 2013

Document Reference:
B100 3 058 13

USE OF SOCIAL MEDIA POLICY

For Employees in Locally Managed Schools

1. Introduction

1.1. The Governing Body of the school is committed to ensuring that all school staff are aware of their responsibilities in connection with the use of social networking sites. It recognises that the use of such sites has become a significant part of life for many people. The purpose of this policy is to ensure that school staff are aware of their responsibilities in connection with the use of social networking sites, and how this may impact on their employment.

1.2. School staff are expected to maintain a professional distance from pupils, and therefore should not be involved in social networking with pupils either in or outside of school.

1.3. The Governing Body believes it important that school staff are able to use technology and related services effectively and flexibly. However, this must be balanced with the Governing Body's duty to safeguard children, the wider community and the reputation of the school.

2. Scope

2.1. This Policy applies to all individuals engaged by the school in a paid or voluntary capacity, including parent helpers, Governors, agency workers, and those on work experience placements (collectively referred to as 'staff' in this policy).

2.2. Staff are expected to comply with this policy at all times to safeguard and protect the privacy, confidentiality and interests of the School, pupils, Local Authority, and the wider school community.

3. Aims

3.1. The policy aims to:

- enable school staff to use social networking sites safely and securely
- ensure that staff are aware of the risks associated with the inappropriate use of social networking sites
- safeguard school staff in connection with the use of social networking sites and to ensure they do not put themselves in vulnerable positions

4. Definition

4.1. For the purposes of this policy, social media are types of interactive online media that allow parties to communicate instantly with each other or to share data in a public forum. This includes, but is not limited to, online social forums such as Facebook, Twitter and LinkedIn. Social media also covers blogs and video and image-sharing websites such as YouTube and Flickr.

4.2. There are many more examples of social media than those listed above, and this is a constantly changing area. Staff should follow these guidelines in relation to any social media that they may use.

5. Use of Social Networking Sites

5.1. All school staff should be aware when using social networking sites that anything said, shown or received could be made available to a wider audience than originally intended. They should follow and understand the following principles.

- Employees and individuals otherwise engaged by the school are not permitted to access social networking sites for personal use via school information systems or school equipment at any time.
- They must not accept pupils as 'friends' and must not approach pupils to become their friends on social networking sites. Personal communication of this nature could be considered inappropriate and unprofessional, and make that individual vulnerable to allegations.
- Any pupil-initiated communication, or online friend requests, must be declined and reported to the Headteacher or designated school child protection colleague.
- Staff are advised not to be online friends with ex or recent pupils of the school or other schools.
- They should not share any personal information with any pupil, including personal contact details, personal website addresses or social networking site details.
- If staff are online 'friends' with any parent/carer linked with the school, they must ensure that they do not disclose any information or otherwise post details which may bring themselves or the school into disrepute. Staff **must not** engage in any online discussion about **any** child attending the school.
- School staff must not disclose, on any social networking site, any information that is confidential to the School, Governing Body, or Local Authority, or post anything that could potentially bring the School, Governing Body or Local Authority into disrepute.
- They must not disclose any personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act.

- Staff should not post photographs of pupils under any circumstances, and should not post photographs of colleagues or others in the school community without their express permission.
- Care should be taken to avoid using language which could be deemed offensive to others.
- Staff are strongly advised to take steps to ensure their online personal data are not accessible to anybody they do not wish to access them. For example, they are advised to check the security and privacy settings of any social networking site they subscribe to and set these to maximum.

6. Breaches of the Policy

6.1. While the Governing Body does not discourage school staff from using social networking sites, staff should be aware that the Headteacher/Governing Body will take seriously any circumstances where such sites are used inappropriately, including any usage that is considered to be online bullying or harassment.

6.2. The Headteacher may exercise her right to monitor the use of the School's information systems, including internet access, where it is believed unauthorised use may be taking place. If such monitoring detects the unauthorised use of social networking sites, disciplinary action may be taken.

6.3 If any instances or allegations of inappropriate use of social networking sites are brought to the attention of the Headteacher/Governing Body, disciplinary action may be taken.

6.4. The Governing Body reserves the right to take action to remove any content posted by school staff which may adversely affect the reputation of the school or the wider school community, or put it at risk of legal action.

Appendix 4
Staff Sanctions

It is intended that incidents of misuse by staff will be dealt with through normal behaviour / disciplinary procedures as follows:

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal	√	√	√	√	√	√	√	√
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	√	√	√		√	√		
Unauthorised downloading or uploading of files	√	√	√		√	√		
Allowing others to access the school network by sharing username and passwords or attempting to access or accessing the school network	√	√	√		√	√		
Careless use of personal data e.g. holding or transferring data in an insecure manner	√	√	√		√	√	√	√
Deliberate actions to breach data protection or network security rules	√	√	√		√	√	√	√
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	√	√	√	√	√	√	√	√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√		√	√	√	√
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	√	√	√		√	√	√	√
Actions which could compromise the staff member's professional standing	√	√	√		√	√	√	√
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√	√		√	√	√	√
Subverting the school's filtering system	√	√	√		√	√	√	√
Accidentally accessing offensive or pornographic material and failing to report the incident	√	√	√		√	√	√	√
Deliberately accessing or trying to access offensive or pornographic material	√	√	√	√	√	√	√	√
Breaching copyright or licensing regulations	√	√	√		√	√	√	√
Continued infringements of the above, following previous warnings or sanctions	√	√	√	√	√	√	√	√