Southfield Primary School E-Safety and Acceptable Use Policy

Contents

Introduction

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment. This policy should be seen in conjunction to the school's Data Protection Policy and compliance with the Data Protection Act 1998. That Act lays down strict rules regarding the processing of personal data, from processing to destruction of both manual and computer records, including visual data such as photographs, relating to identifiable living individuals.

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

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting (Audio Sharing)
- Video Sharing
- Music Sharing / Downloading
- Gaming
- Mobile/Smart phones with functionality including: text, video, web, audio, music , global positioning (GPS)
- Other mobile devices with similar functionality (tablets, laptops, gaming devices)

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

Ensuring children and young people are aware of the risks associated with the use of technologies, and can adopt safer behaviours, is vital in safeguarding them against cyber-bullying and grooming.

At Southfield Primary School we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

This policy relates to both fixed and mobile Internet technologies provided by the school, and technologies owned by pupils, parents and staff, but brought onto school premises.

Roles and Responsibilities

Governors

Governors have ultimate responsibility to ensure:

- The policy and practices are embedded and monitored
- Review the effectiveness of the policy
- They have an understanding of the issues and strategies at the school in relation to local and national guidelines and advice.

Head Teacher and Senior Leaders

- Ensure the E-Safety Policy is disseminated and its importance explained
- All school community have an understanding of the issues and strategies at the school in relation to local and national guidelines and advice.
- Ensure all staff receive suitable and continuing professional development (CPD)

  Ensure all staff are familiar with the procedures to be followed

E- Safety Coordinator and Designated Safeguarding Lead

At Southfield Primary School we have an e-Safety co-ordinator who is also the Designated Safeguarding Lead. This is currently Amandeep Tamber. She will do the following:

- Take day to day responsibility for E-Safety issues
- Ensure all staff understand the importance of the policy and the procedures to follow
- Ensure that staff understand this policy and that it is being implemented consistently throughout the school
- address any online safety issues or incidents
- Ensure that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary

- Keep abreast of current issues and guidance through organisations such as Ealing LA, CEOP (Child Exploitation and Online Protection), UKCCIS (UK Council for Child Internet Safety), and Childnet.
- Ensure new staff receive information on the school's acceptable use policy as part of their induction.

Teaching and Support Staff

- To understand their responsibilities relating to the safeguarding of children within the context of training sessions and The E- Safety policy and know what to do in the event of misuse of technology by any member of the school community.
- To have read, understood and signed the school Staff Acceptable Use Policy
- Be aware of their individual responsibilities to protect the security and confidentiality of school networks, management information 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 logged on or are locked.
- Any confidential data taken off the school premises must be not be taken home on USBs or portable hard-drives.
- Data may only be accessed and used on school computers, laptops, classroom monitor or remotely using RAv3 secure technology. Staff are aware they must not use their personal devices for accessing any school data.
- Staff understand that it is highly inappropriate to use social networking sites and other personal communication tools with pupils and / or parents (e.g. Facebook, MySpace, Twitter, email etc). Staff are expected to use the tools within the school learning platform
- All staff are expected to incorporate activities and awareness within the Computing, PSHE and Relationship Education curriculum areas.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Safeguarding and Child Protection, Health and Safety, home–school agreements, and Behaviour (including the anti-bullying) policy and particularly to the curricula for PSHE and Relationship Education.

Pupils

Pupils are expected to:

- Report abuse, misuse or access to inappropriate materials
- Understand that cyber-bullying is a form of bullying and will not be tolerated
- Safeguard the security of their username and password and not allow other users to access the system using their log in details

Understand the importance of adopting good E-Safety practice

Parent/Carers

We believe that it is essential for parents/ carers to be fully involved with promoting e-Safety both in and outside of school while appreciating the benefits provided by technologies generally. We regularly consult and discuss with parents/ carers and seek to promote a wide understanding about the link between technology and safeguarding.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website)
- The school disseminates information to parents relating to e-Safety where appropriate in the form of:
    - Information and celebration evenings
    - Posters
    - Website
    - Newsletter items

Skills development for staff

- Our staff receive regular information and training on e-Safety issues in the form of E- Safety Co-Ordinator and Computing subject leaders delivering training.

Managing the school e-Safety messages

- We endeavour to embed messages across the curriculum whenever the Internet and/or related technologies are used. This is particularly reinforced in PSHE and Relationship Education lessons in relation to cyber-bullying and to grooming.
- Posters will be prominently displayed in each classroom and in the ICT suite.

- Staff act as good role models in their use of ICT, the internet and mobile devices

Cyber-Mentors

In school we have children from Years 5 and 6 who have been trained as Cyber-Mentors, their role is to be peer mentors and support young people in school with issues relating to bullying, cyber bullying and well-being.

- Cyber - Mentors are on duty during lunch time and children from across the school are able to speak to them about concerns. Cyber Mentors offer them advice and inform a member of staff about their work regularly.
- The aim of having Cyber-Mentors is to inspire and empower young people to help bring communities together

Computing in the Curriculum

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

- The school has a framework for teaching in Computing/ PSHE / Relationship Education lessons. This can be found within the "teacher" drive on the school's network under planning and timetables.
- The school provides opportunities within a range of curriculum areas to teach about Computing and this is achieved through the IPC topics. This can be found within the staff drive under planning and timetables.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Computing /PSHE/Relationship Education curriculum.
- Pupils are made aware of the relevant protocols around using Computing, which may limit what they want to do but also serve to protect them. Children are taught about E-Safety through e-safety presentations in assemblies and through discussions in their lessons.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware 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, or an organisation such as Childline/ CEOP (e.g. through a report abuse button).

- Pupils are taught to evaluate materials critically and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.
- The school's PSHE curriculum provides a set of preventative tools which help safeguard pupils by teaching them about safety on the internet. The school has a comprehensive Relationship Education policy in place which includes the appropriate teaching & learning of:
    - Private and personal space
    - Appropriate / safe and inappropriate / harmful relationships

  In particular, PSHE, SEAL & Relationship Education lessons provide the opportunity to discuss issues relating to cyber-bullying and Internet grooming
- The school refers to the PSHE, Social and Emotional Aspects of Learning, EAL & Relationship Education schemes of work in the PSHE section of the Local Authorities "Healthy Schools room" on the London MLE (Managed Learning Environment)

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. The pupils are expected to keep their passwords secret and not to share with others, not even with their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read ***and sign*** an Acceptable Use Agreement to demonstrate that they have understood the school's policy.
- Users are provided with an individual network, email and Learning Platform log-in user name. From Year 1 they are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If a user thinks their password may have been compromised or someone else has become aware of their password they are expected to report this to their class teacher. This will then be passed on to the Admin team who will then change the password.
- In our school, all ICT passwords are the responsibility of NimbusWeb, the School's ICT support provider, and all staff and pupils are expected to comply with the policies at all times.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the Head teacher with support from the Computing Subject Lead and with guidance from the Local Authority.
- Only staff personnel identified as appropriate by the Head teacher will have remote access to school data.

Managing the Internet

The Internet is an open communication medium, available to all, 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. In our school access to the Internet is via the secure broadband service provided by the London Grid for Learning (LGfL). Internet usage is logged and the logs are randomly but regularly monitored by NimbusWeb, who will check blocked sites that people attempted to access. Whenever any inappropriate use is detected it will be followed up.

- In our school students are not allowed unsupervised access to the Internet.
- Staff will preview any recommended sites before use with students.
- Raw image searches (e.g. Google image search) are discouraged when working with pupils. The LGfL photo gallery is used in class www.gallery.lgfl.net
- If Internet research is set for homework, specific sites will be suggested. These will have been checked by the teacher. Where possible links from the school learning platform will be provided.
- 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.

Infrastructure

- Ealing Local Authority has a monitoring solution via the London Grid for Learning. Upon request, web-based activity can be monitored and recorded.
- School Internet access is controlled through the LGfL's web filtering service.
- Southfield Primary is aware of its responsibility when monitoring staff communication under current legislation and takes into account: the Data Protection Act 1998, Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000 and Human Rights Act 1998.
- Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required.
- The school allows controlled access to Purple Mash and J2E.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the Computing subject leader(s).
- Sophos Anti-Virus protection is provided by the LGfL and is set to automatically update on all school machines. This is the responsibility of network support.
- In addition staff laptops used at home can also be protected by Sophos Anti-Virus as agreed by the LGfL.
- Pupils and staff are not permitted to download programs or files on school equipment without seeking prior permission from the Headteacher or the School's ICT provider, Nimbusweb. If there are any issues related to viruses or anti-virus software, Nimbusweb should be informed via email to the School Business Manager.

Managing other Communication & Networking technologies

The Internet includes a wide range of communication and networking tools & sites. Children need to be educated about appropriate ways of communicating and about the risks of making personal information too easily available. If used responsibly, both outside and within an educational context, it can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school denies access to social networking sites to pupils within school.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, Instant Messaging (IM) email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are asked to report any incidents of bullying to an appropriate adult within school. This will then be recorded and passed on to the Deputy Head with responsibility for Inclusion and Computing subject leader.
- Pupils are introduced to a variety of Internet communication tools within the safe context of the school learning platform / London MLE.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies (such as portable media players, gaming devices, Smart phones, etc) are familiar to children outside of school. Allowing such personal devices to access the school network can provide immense benefits in collaboration, but also create risks associated with misuse, inappropriate communications, etc. Emerging technologies will be examined for educational benefit and the risk assessed before such use of personal devices is facilitated in school. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Staff using their personal devices for school business should make the Headteacher aware of this before doing so.
- Pupils are allowed to bring personal mobile devices/phones to school but these must be handed into the school office in the morning and collected at the end of the day. All devices must be turned off.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed. Capturing images & video is not allowed by students / staff unless on school equipment and for educational purposes.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided mobile devices (including phones)

- The sending of inappropriate text messages between any members of the school community is not allowed.
- School provided mobile devices will be used to record appropriate and relevant images, video or sound recordings .
- Where the school provides mobile technologies (e.g. phones, laptops, etc.) for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Pupil's personal mobile devices (Bring Your Own Devices BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

At Southfield pupils who wish to use their own devices in a school or classroom setting should have a bone-fide reason for doing so i.e. SEN and permission should be received from the Headteacher being going ahead. Where possible all devices used in Southfield Primary School should be provided and managed by the school. Accessories i.e. personal keyboards are allowed in order to facilitate the use of School's equipment where relevant.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff-based or pupil-based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and be aware of what constitutes good 'netiquette'.

- The school gives all staff an individual Legal StaffMail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and that of personal profile information being revealed. When teaching staff communicate with parents and carers by email this correspondence should be sent through the School's email account - admin@southfield.ealing.sch.uk
- 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 email histories can be traced. Staff LGfLmail should be used for all school business.

- Under no circumstances should staff contact pupils or parents or conduct any school business using personal email addresses.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved email accounts on the school system and only under direct teacher supervision for educational purposes.
- LGfL StaffMail and LondonMail are subject to mail scanning.
- Children have their own USO accounts and log on to programs using it.All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive message and keep the offending message(s) as evidence.
- Staff must inform their line manager if they receive an offensive email.
- Pupils are introduced to email in Year 5 through their IPC topic.

Safe Use of Images/Video Taking of Images and Video

Digital images / video are easy to capture, reproduce and publish and, therefore, easily misused. 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 / video by staff and pupils with school equipment.
- Staff are not permitted to use personal devices, (e.g. mobile phones and cameras), to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal devices, (e.g. mobile phones and cameras), to record images of other pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupil's device.

Parents are allowed to take photos / video school events, but are told verbally they must not put on these on the internet.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos/ video 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
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form 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, e.g. divorce of parents, custody issues, etc.
Permissions are stored on SIMS (the School's Management Information System)
Parents/ carers may withdraw permission, in writing, at any time
Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

- Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.
- Video streamed from the LGfL VideoCentral service is always set to "private".

Storage of Images / Video

- Images/ video of children are stored on the school's network under the T drive/planning and timetables/photographs.
- Pupils and staff are not permitted to use personal portable media (e.g. USB storage devices) for storage of images.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform / MLE.

- Nimbus Web have the responsibility of deleting images when specified.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the site manager and the Mechanical and Engineer contractors. Notification of CCTV use is displayed at the front of the school.
- Webcams in school are only ever used for specific learning purposes, (e.g. monitoring hens' eggs). Images of children / adults are broadcast only subject to explicit permission given.
- Misuse of a webcam by any member of the school community will result in sanctions (as listed under the 'Inappropriate Material' section of this document).
    - Webcams can be found in the ICT suite on PCs and built into portable laptops.

Misuse and Infringements

Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Headteacher. Incidents are logged and processes are followed.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the co-ordinator, and depending on the seriousness of the offence may lead to:
    - Reporting to the Child Protection / Safeguarding Officer
    - Investigation by the Head teacher / Local Authority
    - Immediate suspension
    - Dismissal
    - Involvement of police

  Users are made aware of sanctions relating to the misuse of or misconduct in relation to internet technology. This policy has been sent through to all staff and is on the staff website. All staff and pupils and some visitors will have to sign or will be expected to sign an

Acceptable Use Agreement (see appendices) to show they understand and agree to the expectations set out in this policy.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (Also refer to the Anti-Bullying Policy.)

Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes and the issue will be addressed in assemblies.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy and Anti Bullying Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The Designated Safeguarding Lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Equal Opportunities

Pupils with additional needs

The school endeavours to work in partnership with parents to convey a consistent message to all pupils. This in turn should aid the establishment and future development of the schools' rules.

Staff are aware that some pupils will require additional reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Activities are planned to make use of best available resources and are carefully managed for these children and young people.

Reviewing this Policy

Review Procedure

There will be an on-going opportunity for staff to discuss with the coordinator any issue of e-Safety that concerns them.

This policy will be reviewed every 12 months 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.

Related Policies

Staff should refer to the following policies that are related to this E Safety Policy: -

- Information Security Policy
- Data protection Policy.

REVIEW OF POLICY

Governing Body Sub Committee	Published	Review Date	Author
Full Governing body		May 2019	Amandeep Tamber
Headteacher's Signature			
Chair of Governors Signature			

Appendix 1

Southfield Primary School
Staff and Governors - Acceptable Use Agreement Form

The school Acceptable Use Policy is designed to ensure that all staff are aware of their responsibilities when using any form of Information & Communications Technology within their professional role. All staff are expected to sign this policy and adhere at all times to its contents.

- I will comply with the ICT system security protocols and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all my electronic communications with pupils and parents are compatible with my professional role, and never via personal email / phone accounts / social networking profiles.
- I will not discuss school issues on social networking sites / web-blogs.
- I will not give out to pupils, my own personal contact details, such as mobile phone number and personal email address.
- I will only use the approved, secure email system(s) and MLE tools for communications related to my professional role.
- I am aware that communicating with students / pupils via private email / SMS and social networking sites may be considered a disciplinary matter.
- I will ensure that personal data (such as data held on SIMS) 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 and will be encrypted.
- I will not install any hardware or software without permission of the Computing leader.
- I will not browse, download, upload or distribute any material of a pornographic, offensive, illegal or discriminatory nature. I understand that to do so may be considered a disciplinary matter, and in some cases a criminal offence.
- Images & videos of pupils and / or staff will only be taken, stored on school equipment and will only be used for professional purposes in line with

school policy and with written consent of the parent, carer or staff member. Images & video will not be distributed outside the school network / MLE without the permission of the parent/ carer, member of staff 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 or the school into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I have read the full school Acceptable Use Policy and I understand what is expected of me regarding my professional behaviours in the use of technologies.

Signature …… Date ……

Full Name …… (printed)

Job title . . . . . .

Appendix 2

Southfield Primary School
Primary Pupil Acceptable Use Agreement / E-Safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not share my log in details and password with anyone.
- ✓ I will not tell other people my passwords OR use anyone else's.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all Computing 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 arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ 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 e-Safety.
- ✓ I will not give private details (home address, mobile number, email address etc.) to people I meet online.

Child's name:

Class:

Date:

Appendix 3

Southfield Primary School logo and details

Dear Parent/ Carer

Computing including the Internet, email 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. To this end the school has collated a number of rules that children and parents/carers should be aware of when using ICT at home and at school.

Please read and discuss these E-Safety 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 E-Safety Co-ordinator.

✂---

Southfield Primary School: Pupil Acceptable Use Agreement and eSafety Rules – Parent / carer signature

We have discussed this and ……………………………………………(child name) agrees to follow the e-Safety rules and to support the safe use of ICT at Southfield School.

Parent/ Carer Signature …………………….…………………………….

Class ………………………………… Date ………………………………

Appendix 4
Incident Log

A log will be kept by the E-safety Coordinator and all issues acted upon immediately. The teacher with this responsibility is a member of the SLT.

Students / Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).									
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other mobile device									

Unauthorised use of social media / messaging apps / personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school / academy network by sharing username and passwords									
Attempting to access or accessing the school / academy network, using another student's / pupil's account									
Attempting to access or accessing the school / academy network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's / academy'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									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Staff

Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	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 (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data eg 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 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 students / pupils								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy								
Using proxy sites or other means to subvert the school's / academy'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								

Appendix 5
Glossary of terms

AUP Acceptable Use Policy
CEOP Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC Child Protection Committee
CPD Continuous Professional Development
CYPS Children and Young Peoples Services (in Local Authorities)
FOSI Family Online Safety Institute
EA Education Authority
ES Education Scotland
HWB Health and Wellbeing
ICO Information Commissioners Office
ICT Information and Communications Technology
ICTMark Quality standard for schools provided by NAACE
INSET In Service Education and Training
IP address The label that identifies each computer to other computers using the IP (internet protocol)
ISP Internet Service Provider
ISPA Internet Service Providers' Association
IWF Internet Watch Foundation
LA Local Authority
LAN Local Area Network
MIS Management Information System
NEN National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom Office of Communications (Independent communications sector regulator)
TUK Think U Know – educational e-safety programmes for schools, young people and parents.
VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP Wireless Application Protocol