E-Safety Policy

E-Safety Policy
Contents

1. Introduction and overview
    1.1 Rationale and Scope
    1.2 Roles and responsibilities
    1.3 How the policy will be communicated to staff/pupils/community
    1.4 Handling complaints
    1.5 Review and Monitoring

2. Education and Curriculum
    2.1 Pupil e-safety Curriculum
    2.2 Staff and governor training
    2.3 Parent awareness and training

3. Expected Conduct and Incident Management
    3.1 Expected Conduct
    3.2 Incident Management

4. Managing the ICT infrastructure
    4.1 Internet access, security (virus protection) and filtering
    4.2 Network management (user access, backup, curriculum and admin)
    4.3 Passwords policy
    4.4 E-mail
    4.5 School website
    4.6 Learning platform
    4.7 Social networking
    4.8 CCTV

5. Data security: Management Information System access and data transfer

6. Equipment and Digital Content
    6.1 Personal mobile phones and devices
    6.2 Digital images and video
    6.3 Asset disposal

Appendices:
1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement Mobile Phones (Staff)
3. Acceptable Use Agreement (Pupils)
4. The use of Social Networking and on-line media

1. Introduction and Overview

1.1 Rationale and Scope

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Southborough Primary School with respect to the use of ICT-based technologies
- safeguard and protect the children and staff of Southborough Primary School
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content.

Contact

- grooming (sexual exploitation, radicalisation etc.)
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online - internet or gaming)
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film).

Commercialism

- spam, pop-up windows, unwanted commercial contact.

Scope

This policy applies to all members of Southborough Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

1.2 Roles and Responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g LGfL • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident • To receive regular monitoring reports from the E-Safety Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager).

ICT Manager	• To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• To promote an awareness and commitment to e-safeguarding throughout the school community
	• To ensure that e-safety education is embedded across the curriculum
	• To communicate regularly with SLT and the designated e-Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an e-safety incident log is kept up to date
	• To facilitate training and advice for all staff
	• To liaise with the Local Authority and relevant agencies
	• To regularly update in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media.
	• To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which

Role	Key Responsibilities
	passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • To ensure that the school's policy on web filtering is applied and updated on a regular basis • To ensure that LGfL is informed of issues relating to the filtering applied by the Grid • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
Governors / E-safety governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors' Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: • regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs).
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly.
School Business Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place.
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts.
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD

Role	Key Responsibilities
	• To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• To read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (note: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • to help the school in the creation/ review of e-safety policies.
Parents/carers	• to support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website / LEARNING PLATFORM / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement • to consult with the school if they have any concerns about their children's use of technology.
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school.

1.3 Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- being posted on the school website
- being part of school induction pack for new staff
- Acceptable Use agreements discussed with pupils at the start of each year.
- Acceptable Use agreements to be issued to whole school community, usually on entry to the school
- Acceptable Use agreements to be held in pupil and personnel files.

1.4 Handling complaints:

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by a member of staff / e-Safety Coordinator / Headteacher
  - informing parents or carers
  - removal of internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework)
  - referral to LA / police.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

1.5 Review and Monitoring

The e-safety policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

2.1 Pupil e-Safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA / LGfL e-Safeguarding and e-literacy framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
    - to know how to narrow down or refine a search
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour
    - keeping personal information private
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
    - to understand why they must not post pictures or videos of others without their permission
    - to know not to download any files – such as music files - without permission
    - to have strategies for dealing with receipt of inappropriate materials
    - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons
    - to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
    - to know how to report any abuse including cyberbullying; and how to to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.

2.2 Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- Makes regular training available to staff on e-safety issues and the school's e-safety education programme
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e- safeguarding policy and the school's Acceptable Use Policies.

2.3 Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - information leaflets; in school newsletters; on the school web site
    - demonstrations, practical sessions held at school
    - suggestions for safe internet use at home
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

3.1 Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (At KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- need to understand the importance of misuse or access to inappropriate materials and to be aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers
- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

3.2 Incident Management

In this school:
- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes
- support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible
- We will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

4. Managing the ICT infrastructure

4.1 Internet access, security (virus protection) and filtering

This school:
- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of anti-virus software etc and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;

- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved learning platform
- Only unblocks other external social networking sites for specific purposes / internet literacy lessons
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns
- Ensures pupils only publish within an appropriately secure environment : the school's learning environment/ the London learning platform / LGfL secure platforms
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's learning platform as a key way to direct students to age / subject appropriate web sites
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search
- Informs all users that internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the e-Safety Coordinator. Our system administrator(s) logs or escalates as appropriate to the technical service provider or LGfL Helpdesk as necessary
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – police – and the LA.

4.2 Network management (user access, backup, curriculum and admin)

This school

- Uses individual, audited log-ins for all users - the London USO system
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services

  Storage of all data within the school will conform to the UK data protection requirements

  Pupils and staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety policy. Following this, they are set-up with internet, email access and network access. Online access to service is through a unique, audited username and password
- Ensures staff access to the school's management information system is controlled through a separate password for data security purposes
- Uses the London Grid for Learning's Unified Sign-On (USO) system for username and passwords
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves
- Has set-up the network so that users cannot download executable files / programmes
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure health and safety regulations are is followed;
  e.g. projector filters cleaned; equipment installed and checked by approved suppliers / Local Authority electrical engineers
- Has integrated curriculum and administration networks, but access to the management information system is set-up so as to ensure staff users can only access modules related to their role:
  e.g. teachers access report writing module; SEN coordinator - SEN data
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems: e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child
- Provides pupils and staff with access to content and resources through the approved learning platform which staff and pupils access using their username and password (their USO username and password)
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files

- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external audit's requirements
- Uses our broadband network for our CCTV system and have had set-up by approved partners
- Uses the DfE secure s2s website for all CTF files sent to other schools
- Ensures that all pupil level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX)
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- Ensures that our wireless network has been secured to industry standard Enterprise security level / appropriate standards suitable for educational use
- Ensures that all computer equipment is installed professionally and meets health and safety standards
- Ensures that projectors are maintained so that the quality of presentation remains high
- Reviews the school ICT systems regularly with regard to health and safety and security.

4.3 Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

4.4 E-mail

This school

- Provides staff with an email account for their professional use, through LGFL staff mail and makes clear personal email should be through a separate account
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example admin@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public
- Will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the world wide web.

Pupils:

- Pupils are introduced to and use e-mail as part of the ICT/Computing scheme of work.
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home, i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and who is approved by their teacher or parent/carer
    - that an e-mail is a form of publishing where the message should be clear, short and concise
    - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
    - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe
    - that they should think carefully before sending any attachments
    - embedding adverts is not allowed
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature
    - not to respond to malicious or threatening messages
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying
    - not to arrange to meet anyone they meet through e-mail without having discussed it with an adult and taking a responsible adult with them
    - that forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':

- the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used
- the sending of chain letters is not permitted
- embedding adverts is not allowed.

- All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

4.5 School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- Uploading of information is restricted to our website authorisers
- The school web site complies with the statutory DfE guidelines for publications
- Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address and telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published
- Children's photographs published on the web do not have full names attached
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website
- We do not use embedded geodata in respect of stored images
- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

4.6 Learning platform

- Uploading of information on the school's learning platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas
- Photographs and videos uploaded to the school's learning platform will only be accessible by members of the school community
- In school, pupils are only able to upload and publish within school approved and closed systems.

4.7 Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the school's preferred system for such communications.
- The school's preferred system for social networking will be maintained in adherence with the communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff

- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or Local Authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

4.8 CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the support provider for 28 days*), without permission except where disclosed to the police as part of a criminal investigation.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Headteacher is the Senior Information Risk Officer (SIRO)
- We ensure staff know who to report any incidents where data protection may have been compromised
- All staff are DBS checked and records are held in one central record
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  - staff
  - governors
  - pupils
  - parents

  This makes clear staff's responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal
- School staff with access to setting-up usernames and passwords for email, network access and learning platform access are working within the approved system and follow the security processes required by those systems.

6. Equipment and Digital Content

6.1 Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's and parent's or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- The school strongly advises that student mobile phones should not be brought into school. Should a mobile phone be seen, whether being used for calls, texts, to take photos or just to show to other children it will be confiscated and it will need to be collected by the parent/carer. Parents are regularly reminded of the school's policy via the website and newsletters.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

6.2 Digital images and video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make personal information public.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Appendix 1

Southborough Primary School

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (This is currently: LGFL Staff mail)
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will access school resources remotely (such as from home) only through the LGfL / school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will alert the school's named child protection officer / relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): Staff agreement form

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

School .....

Authorised Signature (Head Teacher

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

Appendix 2

ACCEPTABLE USE POLICY MOBILE PHONES – STAFF

Southborough Primary School

Acceptable Use Policy (AUP): Staff agreement form

Use and storage of mobile phones in school

- I will switch my mobile phone off or on silent mode while in school
- I agree to store my mobile phone in a locker or bag in a secure place where children will not be able to see or potentially have access to it
- I will not have my mobile phone in my pockets or on my person unless there are exceptional circumstance and I have had permission from the Head Teacher
- When on school/class trips, I will leave my mobile phone in a secure place at school unless prior permission has been given from Head Teacher
- The schools mobile phones will be used while on trips to communicate with school, parents or colleagues
- I will not use my mobile to take photos or videos of pupils or colleagues unless it has been previously agreed with the Head Teacher
- I understand that I can only check or make phone calls on my mobile phone at break or lunch times and that this should only be done in the staff room or in one of the offices within the school
- I understand that if a family member or other needs to contact me in an emergency they should do so by phoning the school office
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school
- I understand that failure to comply with this agreement could lead to disciplinary action

The school understands and acknowledges that in certain extenuating circumstance staff need to have immediate access to their mobile phones and this will be considered and agreed on an individual basis.

User Signature

I agree to abide by all the points above.

Signature .....Date.....

Full Name ..... (printed)

Job title .....

School .....

Appendix 3(a) Acceptable Use Agreement KS1

S

I will only use the Internet and email with an adult

A

I will only click on icons and links when I know they are safe

F

I will only send friendly and polite messages

E

If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

Appendix 3 (b)

Southborough Primary School
KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

Name: *Class:*

Appendix 4

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/browser-safety/