Barbara Speake Stage School

Barbara Speake Stage School
E-Safety Policy

Contents

Appendices:

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils)
3. Acceptable Use Agreement including phot/video permission (Parents)

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at The Barbara Speake Stage School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of The Barbara Speake Stage 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 polices.
- 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 summarized 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
- Cyber-bullying in all forms
- Identify 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)
  (ref Ofsted 2013)

Scope (from SWGfL)
This policy applies to all members of The Barbara Speake Stage 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 The Barbara Speake Stage School.

The Education and Inspections Act 2006 empowers Head teachers/Principals to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Head teacher	• To take overall responsibility for e-Safety provision. • To take overall responsibility for data and data security (SIRO). • 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 ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager/Head Teacher)
e-safety Co-ordinator/ Designated Child Protection Lead	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents. • Promotes an awareness and commitment to e-safeguarding throughout the school community • Ensures that e-safety education is embedded across the curriculum

	• To communicate regularly with SLT 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.
	• Facilitates training and advice for all staff.
	• Liaises with the Local Authority and relevant agencies
	• Is regularly updated 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

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 Head Teacher receiving regular information about e-safety incidents and monitoring reports. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities. • The role of the E-Safety monitoring will include: • Regular review with the e-safety co-ordinator/ officer (including e-safety 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.
Network Manager/ technician	• To report any e-Safety related issues that arises, to the e-Safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which 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. • The school's policy on web filtering is applied and updated on a regular basis • That he/she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • That the use of the *network/remote access/email* is regularly monitored in order that any misuse/attempted misuse can be reported to the *E-Safety Co-ordinator/ Officer/ Head teacher for investigation/ action/ sanction.* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place.
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 contents 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 • 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. Personal email, Personal text, Personal mobile phones etc.

Pupils	• Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy (nb. At KS1 it would be expected that parents/carers would sign on behalf of the pupils). • 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.
Notice for parents	• Educating Parents and raising e-safety awareness.
Parents/Carers	• To support the school in promoting e-safety and endorse the Parent's 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/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.

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

- Policy to be distributed to all staff via individual USB's & displayed in the Junior ICT/Art Room, Staff Study & Staff Room
- Policy to be part of the school induction pack for new staff
- Acceptable us 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

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 not 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 by tutor/Head of Year/ Head teacher
    - 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.
- Our e-safety Coordinator acts as first point of contact for any complaint. Any compliant about staff misuse is referred to the Head teacher.
- 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 child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other school policies, Child Protection policy, Anti-Bullying policy & Behaviour Policy.

- The school is to be responsible for document ownership, review and updates.
- The e-safety policy will be reviews 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 by the SLT 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. All amendments to the school e-Safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

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 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 website/ 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 see help if they are affected by any form of online bullying.
    - To know how to report any abuse including cyberbullying; and how 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 organization such as ChildLine.

- 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.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons and breaks.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also known 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 online, online gaming and gambling.

Staff 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 program.
- Provides as art 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.

Parent awareness and training

This school

- Runs a rolling programme of advice and guidance 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
    - Suggestions for safe internet use at home;
    - Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users;

- Are responsible for using 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 are 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 god 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.

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 (e.g. 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 and 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

Internet access, security (virus protection) and filtering

This school:

- 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 understand that they must report any concerns.
- Ensures pupils only publish within an appropriately secure environment.
- Requires staff to preview websites before use [where not previously viewed or cached]. Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open internet searching is required; e.g. yahoo for kids or ask for kids, Google Safe Search,…
- Never allows/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 they must report any failure of the filtering systems directly to the SLT who will then log the failure.
- 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.

Network management (user access, backup)

This school

- 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.

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.
- 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 off-on again as themselves. Requests that teaches and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers, projectors and smart boards off at the end of every day.
- 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 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.
- *Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;*
  e.g. borough email or intranet; finance system, personnel system etc.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned and equipment installed and checked by approved suppliers.
- 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.
- Uses the DfE secure S2s website for all CTF files sent to other schools.
- 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.
- All computer equipment is installed professionally and meets health and safety standards.
- 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.

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 other can find.

E-mail

This school

- Provides staff with an email account for their professional use.
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- 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 desktop anti-virus product Norton, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Pupils:

- Pupils are introduced to and use e-mail a part of the ICT/Computing scheme of work.

- 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 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 email 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 email, 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 email 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 emails, but to keep them as evidence of bullying.
    - Not to arrange to meet anyone they meet thorough email without having discussed with an adult and taking a responsible adult with them.
    - That forwarding 'chain' email letters is not permitted.

- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.

Staff:

- Access in school to external personal email accounts may be blocked.
- Staff know that email sent to an eternal organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That is 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 school Agreement Form AUP to say they have read and understood the e-safety rules, including email and to explain how any inappropriate use will be dealt with.

School website

- the head teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.

- Most material is the school's own work; where other's work is published, or lined to, we credit the source used and state clearly the author's identity or status.
- The point of contact on the website is the school address, telephone number and we use a general email contact address, 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.

Social networking

- Techers 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 schools' preferred system for such communications.

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/* local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

5. Data security: Management Information System access and Data transfer
Strategic and operational practices

At this school:

- The head teacher is the Senior Information Risk Office (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 register.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professional working in the Local Authority or their partners in Children's Services/Family Services, Health Welfare and Social Services.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which no longer need to be stored.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- All students must hand in their mobile phones fully switched off and not on silent and any other electronic equipment before morning assembly. These

items will then be returned to the students at the end of the school day. (See separate: Behaviour, Class Room Management & Exclusion Policy).

- Staff members may use their phones during school break times, however only in designated areas, (staff room & Staff Study) never in any classroom, studio or corridor. They must also be switched off at all other times. All visitors are requested to keep their phones on silent.
- 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 SLT. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the SLT 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 the 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, however this must be in a staff allocated area, as stated above. 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 at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Students are not permitted to use mobile phones or any other personal electronic equipment capable of connecting to the internet and or recording still or moving images anywhere in the building.
- 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 and personally owned devices should not be brought into school. If, however a student brings any mobile device in to school, they must be handed in to the office for safe keeping before morning assembly and handed back after the afternoon assembly in line with the schools Behaviour, Class Room Management and Exclusion Policy (see separate policy)
- The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school Behaviour, Classroom Management and Exclusion Policy then the phone or device will be confiscated and will head in a secure place in the school office, until a parent comes to collect the item.

Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examinations or all examinations.

- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. 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 and never outside of the staff allocated areas, unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned deice as part of an educational activity then it will only take place when approved by the senior leadership team, by written authorisation.
- Staff should not use personally-owned devices, such a 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 make 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.

Digital images and video
In this school:

- We gain parental/carer permission for sue of digital photographs or video involving their child as part of the school agreement form when their child 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.
- Pupils are taught about how images can be manipulated in their eSafety 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 perianal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

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.

Date Published: September 2017 **Review date:** September 2018

This policy will be reviewed annually.

Barbara Speake Stage School

E-Safety agreement form: Parents

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my daughter/son access to:

- The internet at school
- ICT facilities and equipment at the school

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs/video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the internet and digital technology at home. I will inform the school if I have any concerns.

My daughter/son name(s): _____

Parent/guardian signature: _____

Date: ___ / ___ / _____

Barbara Speake Stage School

The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings if your daughter/son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.
If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
Only images of pupils in suitable dress are used.
Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity; e.g. taking photos or a video of progress made a nursery child, as part of the learning record and then sharing with their parent/guardian.
- Your child's image being used for presentation purposes around the school; e.g. in class or wider school wall displays or PowerPoint © presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. within a CDROM/DVD or a document sharing good practice; in our school prospectus or on our school website. Your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

  Note: if we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

  The use of social networking and online 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 website 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 ant they provide robust mechanisms to report contact or activity which braches 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

Barbara Speake Stage 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: 1and1)
- 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 resource 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 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 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 on 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

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 (SLT)
I approve this user to be set-up.

Signature Date

Full name (printed) _____

Barbara Speake Stage School
KS3 & KS4 Pupil Acceptable Use Agreement

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

1. I will only use the school's computers for schoolwork, homework and as directed.
2. I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace. I will only edit or delete my own files and not view, or change, other people's files without their permission.
3. I will keep my logins, IDs and password secret.
4. I will use the internet responsibly and will not visit websites I know to be banned by the school. I am also aware that during lessons I should visit websites that are appropriate for my studies.
5. I will only e-mail people I know or those approved by my teachers.
6. The messages I send or information I upload will always be polite and sensible.
7. I will not open attachments or download a file unless I have permission or I know and trust the person that has sent them.
8. I will not give my home address, phone number, send photographs 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.
9. I will never arrange to meet someone I have only ever previously met on the internet or by email or in a chat room, unless I take a trusted adult with me.
10. 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 save it and talk to a teacher/trusted adult.
11. I am aware that some websites and social networks have age restrictions and I should respect this.
12. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.

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

Signed: Date:

Name (printed): _____

Barbara Speake Stage School

KS1 & 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 without their permission.
- I will keep my logins and password secret.
- I will not bring files into school without permission or upload inappropriate material to my workplace.
- 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 email 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:
(parents signature on behalf of KS1)

Name (printed): _____