Swaffham Bulbeck Church of England Primary School
E-Safety Policy

Last reviewed:	February 2017
Next review due by:	February 2020

1. Introduction

1.1 Background to this policy:
The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to e-safety, including:

- The policies and practice embedded in our school and followed by the whole school community.
- A progressive, age appropriate e-safety curriculum for all pupils. E-safety in schools is primarily a safeguarding and not a computing / technology one.
- The infrastructure and how it is set up to keep pupils safe online, including monitoring, and preventing and responding to e-safety incidents.

1.2 Therefore this policy should be viewed alongside other Safeguarding policies and guidance including, but not limited to:
Staff handbook
Code of conduct
Safeguarding and Child Protection policy
Personal Social and Health Education (PSHE)
Safer Working Practices
Data Protection Policy
Anti-Bullying Policy
School Complaints Procedure
Cambridgeshire Progression in Computing Capability Materials
Whistle Blowing Policy

1.3 The purpose of internet access and communication technology in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. Exploring and using the online world is a key way of extending and personalising the educational experience of all learners.

1.4 'Staff' in this document is defined as any adults regularly working or volunteering in school, especially those given access to computer systems in the school, and includes employees, trainees, governors and volunteers. All those allowed computer access must sign a copy of the school's *ICT Acceptable Use Statement* (Appendix A) and submit it to the school office to show their agreement to abide by this policy. In addition all visitors to the school will be asked to agree to key requirements in the visitor's code of conduct (See Appendix B).

1.3 The following sections of this policy actively promote our school's response to the government's anti-terrorism Prevent Strategy: 2.8 logging of e-safety incidents; 3 internet filtering; 8.4 social networking; 15 sanctions.

2. **Teaching and Learning of E-safety**

2.1 At the beginning of each academic year pupils in KS1 & KS2 are reminded about the pupil's Acceptable Use Agreements. They are asked to sign their agreement to these and a copy is sent home for discussion with parents/carers (See Appendix C).

2.2 The 2014 National Curriculum Computing objectives relating to e-safety are to:
- KS1: *use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies;*
- KS2: *use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.*

2.3 At KS1, planning provides practical opportunities for pupils to be actively taught:

- what constitutes respectful communication when using email, forums, online games etc;
- what counts as personal information and how to keep this private;
- that people messaging and authoring online are able to mask their true identities;
- to tell a teacher, parent or trusted adult immediately if they encounter any material or contact that makes them feel uncomfortable.

2.4 At KS2, planning provides practical opportunities for the points above to be covered at a more sophisticated level, plus practical applications for children to consider:
- ways in which the internet is a tool that can be used responsibly for good but also to cause harm;
- how to report concerns online, beyond telling a trusted adult;
- ways to validate information before accepting that it is necessarily accurate;
- to acknowledge the source of information, when using Internet material, including copyrighted images, for their own use.

2.5 In delivering the wider curriculum, teachers will plan for and make use of communication technology. Primarily, this will be through Starz+, a personalised learning platform which includes:
- personal and class email accounts (limited to Swaffham Bulbeck Church of England Primary School users);
- forums and chat-rooms (limited to Swaffham Bulbeck Church of England Primary School users);
- video conferencing;
- other suitable and, if necessary, risk-assessed web-based resources.

2.6 At Swaffham Bulbeck Church of England Primary School we believe that a comprehensive programme of e-safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

This is achieved using a combination of discrete and embedded activities drawn from a selection of appropriate materials including the ACE (Accredited Competence in E-safety) scheme of work and is linked to our online learning platform, Starz+.

Our programme for e-safety education is evidenced in teachers' planning either as discrete or embedded activities.

Key e-safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in discussion forums.

2.7 The designated person for child protection is responsible for keeping a log of all known **e-safety incidents**, involving any members of the school community, in or out of school. E-safety incidents are defined as those putting a child's safeguarding or wellbeing at risk. Examples include: cyber-bullying; filtering failures resulting in inappropriate search results; inappropriate use of digital technologies and/or the internet, to promote opinions or views which are against the aims of the school. Such incidents are always taken seriously, acted on accordingly and passed on to other agencies when necessary. When concerning pupils, the parents/carers of all involved will be informed. Incidents and following actions are monitored regularly by the e-safety group and any lessons learnt lead to changes in policy, which are then shared with staff.

3. Internet Filtering

3.1 Cambridgeshire LA, through *The ICT Service*, provides the school's internet access. This is filtered by the *Lightspeed* web-filter, denying access to inappropriate sites. There are two levels of filtering; one for staff and one for pupils. For this reason, pupils should only use devices logged on as a pupil.

3.2 The school can request specific websites be whitelisted or blacklisted by contacting The ICT Service helpdesk. If staff become aware of inappropriate material by-passing the filter, this must be reported to the Headteacher or ICT subject leader as soon as possible, who will pass on the information to The ICT Service helpdesk.

3.3 Previously unused websites or apps must be thoroughly checked by staff before children are allowed access. Particular care must be taken with sites or Apps containing potentially inappropriate advertising (eg, YouTube).

3.4 The class teacher, club-leader or TA will always supervise pupils when online and will take all reasonable precautions to ensure that users access only appropriate material. Due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a screen and the school cannot accept liability for the material accessed.

3.5 The use of computer systems without permission, or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

4. **Management of pupils' Starz+ accounts**

4.1 The following principles will apply:

- Pupils will be given individual Starz+ accounts which can be used to send and receive email and messages in school and beyond, but only to other Swaffham Bulbeck Church of England Primary School Starz+ users.
- They will be actively taught how to use these accounts appropriately and safely.
- Pupils can only send emails outside the school domain by going through the class email account. All <u>return</u> emails have to go to the class address, unless specifically set up by the teacher, eg, for communication with a paired school that is also in the Starz community.
- Starz+ automatically flags up bad language to the child's class teacher for them to investigate.
- Children can report bullying or inappropriate behaviour by clicking a red flag. They will be actively taught how to use this appropriately.
- Supervising staff will occasionally monitor messages received and sent by pupils. Pupils will be made aware of this.
- If a child is found to have been using their Starz+ account inappropriately, they will be warned that access will be blocked if the behaviour continues. They will then be closely monitored by the class teacher.

5. Chatrooms, forums & multi-user online games

5.1 Chatrooms, forums and online games, etc, allow children to communicate with others online. Forums and wikis can be accessed through Starz+. If teachers want to make use of other websites or Apps, allowing online communication with those outside of the school community, a risk assessment must be signed by the Headteacher. Un-moderated sites are not allowed to be used.

6. Staff use of Email

- Email messages must be treated like any other formal written communication. Email messages cannot be considered to be private, secure or temporary.

- Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

- Email messages, however confidential or damaging, may have to be disclosed in court proceedings. Staff must not create or send email messages that may be intimidating, hostile or offensive, including on the basis of gender, race, sexual orientation or any other characteristic covered by the Equalities Act 2010.

- Improper statements in email can give rise to personal liability and liability for Swaffham Bulbeck Church of England Primary School or the Cambridgeshire LA and can constitute a serious disciplinary matter. Emails that embarrass misrepresent or convey an unjust or unfavourable impression of the school or LA or its business affairs or employees are not permitted.

- It is never permissible to subject another employee to public humiliation or ridicule; this is equally true via email.

- Copyright law applies to email. Do not use email to transmit or circulate copyrighted materials, including images.

- Emails containing personal information about pupils or other members of the school community can only be sent without encryption to addresses linked to the Local Authority, e.g., those ending '*cambs.sch.uk*' or '*cambridgeshire.gov.uk*' .

7. **The School Web-Site**

7.1 The following points also apply to all documents uploaded to the website.

- The point of contact on the website is the school address, email and telephone number. Home information or individual email identities will not be published.
- Photographs will only be used of children whose parents/guardians have not requested otherwise.
- All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name. This includes images.
- Pupils' photos are never used alongside their full-names.

8. Social networking

8.1 There is often an age limit for these sites, but this is not enforced by the owners and therefore children can access them and may have accounts. For this reason, social networking is included when teaching e-safety in KS2.

8.2 Staff must never accept friendship requests from pupils at the school and will only accept friendship requests from pupils' adult family members if they socialise with them outside of school. Staff must be aware that members of the school community may be 'friends of friends' and as such may be able to access information on their timeline. Personal security settings must be set to take this into account and one's own professional standing must be protected through what is allowed to be seen online.

8.3 Staff must never publish any information on social networking sites about pupils at the school or members of their families. Staff and pupils must not bring the school, or members of the school community, into disrespect by publishing material on the internet.

8.4 Staff must ensure that opinions expressed online do not undermine fundamental British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs

8.5 If employees of the school are found to have acted inappropriately online this will be dealt with through the school's *Misconduct Policy*. If volunteers or trainees are found to have acted inappropriately online this will be investigated by the Headteacher, who may issue a warning or ask them to cease activity within school immediately.

9 Security of school ICT systems

9.1 The Internet is a connection to the outside world that could compromise system performance or threaten security. The system will be maintained as follows:-

9.2 Security strategies follow recommendations made by the LA:

- The security of the whole system is regularly reviewed by the ICT technician.
- Virus protection is installed and updated regularly, directly through the internet.
- All files and folders will be saved in appropriate folders on the school network, rather than local machines. Folders saved on the hard drives of the machines will not be backed up on the network.
- PC's and laptops will be disposed of securely, according to LA recommendations at the time.
- Memory sticks will be subject to virus checks and must not be used if Sophos (the LA virus checker and firewall) indicates there is a problem. Children will be encouraged to save their work in Starz+ in order to bring work into school, rather than use memory sticks.

9.3 **Logins and Passwords:**

- All PC's are configured to present an authentication challenge on start up. This has been simplified in order to enable easier access by children.
- All school staff (including non-teaching staff) are issued with their own unique user ID and password to ensure there is accountability and an audit trail of their activities.
- Staff must never divulge their passwords to anyone, except the Headteacher or technician, and then, only when necessary. Passwords protect the school systems from access by unauthorised people: they protect your work and the school information.
- Procedures are in place to ensure users change passwords initially and on a regular basis.
- Passwords are of a minimum length and old passwords cannot be re-used immediately.
- Children use a year group login to access PC's. They have individual ID's to access online materials such as Starz+. Care needs to be taken to log off at the end of the lesson to prevent unauthorised access.
- School will ensure that only those with a genuine need to access systems are provided with user ID's.
- Master/Administrator passwords are only given to those with a genuine need for them. Care is taken to ensure these are kept secret and they are changed regularly.

9.4 **Software**

Only software properly purchased and/or approved by the school may be used on school PCs and laptops. Non-standard or unauthorised software can cause problems and it is advisable to check with the Headteacher or ICT technician before the installation of such software. Software or shareware may be downloaded from the Internet or loaded from other sources (e.g. CDROM) when necessary, however it is the responsibility of the individual to ensure that any licensing issues are addressed promptly, either by on-line registration or the purchasing of a valid licence. The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licences must always be adhered to.

Whilst it is the user’s responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above must contact the technician or ICT helpline who will be happy to assist in resolving any issues.

9.5 **Data Security**

Information held on the school’s computer systems must only be accessed by those who have been properly authorised to do so and who need the information to carry out their work. Under no circumstances should personal or other confidential information held on a computer be disclosed to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers’ Misuse Act 1990.

It is school policy to store data on a network drive where it is regularly backed up. You must ensure that data that is not stored on the network file server is regularly backed up.

Personal data shall be:

- obtained processed fairly and lawfully;
- held for specified lawful purpose(s);
- not used or disclosed in a way incompatible with the purpose(s);
- adequate, relevant and not excessive for the purpose(s);
- accurate and up to date;
- not kept longer than necessary;
- available to the data subject;
- kept secure through password protected files or encryption.

10 Monitoring Internet Use

10.1 At a county level the school’s filter log will be analysed for evidence of child sex abuser key words. A report will identify date and time of any blocks together with the unique user ID.

11 **Action to be taken if misuse is suspected.** Schools must never investigate such cases themselves but observe the following procedure:

<u>Evidence must be immediately secured</u>

- The PC/Device should be immediately powered down and removed from service.
- The police must be contacted immediately via CEOP: <u>www.ceop.police.uk/safety-centre/</u>
- Arrangements will be made to collect the PC/device for forensic examination.
- Schools should never attempt to access a site which they believe to be illegal – to do so would technically break the law and make them liable to prosecution. Staff should trust their judgement and quarantine the PC/device without undertaking any investigations of their own.
- If there is any doubt about the subject matter, it is enough to view the internet history. Any attempt to follow the internet hyperlinks to the sites themselves will invalidate evidence by updating the time stamps of images received.

12 Staff laptops

- The laptops are the property of the school and are primarily for delivering school work and not for the storage of personal family photographs, movies or music, etc.
- Family and friends are not allowed to use the school equipment at all (this is to protect the member of staff as much as the school).
- The member of staff is responsible for maintaining the secrecy of their own password and this must not be divulged to anyone else (including colleagues, pupils or members of their family).
- They will be held responsible for any misuse of the laptop issued to them.
- Central hosting key fobs remain the property of the school and must be returned on leaving the school.
- Staff must not store any personal data of children or staff on memory sticks unless these are encrypted. Scans for viruses should be done regularly on memory sticks that are used between home and school.
- Staff laptops need to be kept secure when school is closed, ideally taken off the premises. They must not be left in locked cars.
- When a member of staff ceases to hold a laptop (when leaving employment or when upgrading) the laptop will be given to the ICT technician for data to be wiped.

13 Virus Protection

13.1 Anti-virus software is loaded on all computers as standard and is updated regularly via the network. Anti-virus software must not be de-installed or deactivated. Files received by or sent by email are checked for viruses automatically. Users must not intentionally access or transmit computer viruses or similar software.

14 Personal devices

14.1 See section 7.2 of the school's '*Safeguarding & Child Protection Policy*'. '*Use of Mobile Phones in School Policy*' (see Appendix D) details the school's approach to phones brought in to school.

14.3 Once governors have signed the acceptable use statement (Appendix B) they can be given the wireless access key. This is to enable governors to view and edit documents through the Starz VLE using their own personal devices whilst on site.

14.4 Pupils are permitted to bring their own mobile devices into school, with the permission of their class teacher and assumed permission of a parent/carer, and with good reason. The school cannot accept responsibility for loss or breakage in these cases. As long as the class teacher is able to monitor usage in the same way they would monitor school mobile devices, Pupils must not, however, be told wifi passwords. The internet must not be accessed via a phone network (3G/4G), thereby bypassing web-filtering. Pupil devices with this capability must have it disabled when in school.

14.5 If pupils, staff or visitors are found to have used personal devices inappropriately they will not be allowed to bring them into school in the future. An initial warning may be issued before this sanction is actioned. Misuse of personal devices must be reported to the Headteacher as soon as possible.

14.6 If it is felt that an adult has misused a personal device, this should be dealt with in line with the whistleblowing policy; the Headteacher or another senior member of staff must be informed.

15 Sanctions

15.1 Non-compliance with any aspects of this policy will be treated seriously and investigated appropriately by the Headteacher, governing body and/or other agencies. Matters involving employees of the school will be dealt with in line with the school's Disciplinary Procedures. Volunteers or other adults working in school (depending on the seriousness of the offence) may be warned, denied access to school systems and equipment, asked to cease activities in school or reported to the police.

16 **Policy Review**

16.1 This policy will be reviewed annually, or when necessary and will include consultation with pupils, staff, governors and parents.

Appendix A

ICT Acceptable Use Statement

By signing below I agree to actively promote e-safety at Swaffham Bulbeck Church of England Primary School by keeping to all points as set out in the school's e-safety policy.

Name	**Signature**	**Date**

Appendix B

Code of conduct for all visitors

Swaffham Bulbeck Church of England Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all adults onsite to share this commitment.

The following must be complied with by all visitors onsite when school is open to children:

• All regular visitors must have DBS safeguarding check details logged with office staff. They must also sign to show their agreement with our safeguarding policies.

• Visitors who are not regular may not require DBS clearance but must not be with children without an accompanying member of school staff, unless specific permission has been given by the Head teacher.

• Mobile phones are not to be used in any areas where children are present or could be. This includes phone calls, texting and photographing. If a visitor or parent/carer is seen using their mobile phone, they will be asked politely to turn it off/desist from using it/remove it from children’s view.

• All visitors must wear a visitor’s badge and sign-in whilst on-site.

• Visitors must avoid physical contact with a child other than for reasons of safety.

• If it is necessary to be alone with a child this must be in an area visible to onlookers (e.g. a room with a windowed door).

Appendix C

Early Years and KS1 E-safety Acceptable Use Agreement

• I will normally only use the school's ICT equipment and tools (including computers,cameras, Starz etc.) for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.

• I will only use the internet and email when an adult is nearby.

• I will not share my passwords with other people and will tell my teacher if I think someone else knows them.

• I will ask a responsible adult before opening an email from someone I don't know.

• I will not share details about myself such as surname, phone number, home address and photograph.

• I will ask for permission if I need to look at other peoples' work on the computer.

• I will try my hardest to only send messages which don't upset other people.

• I will ask my teacher before using photos or video.

• If I see something on a screen which upsets me, I will always tell an adult.

• I will do my best to follow these rules at both home and school because I know they are there to keep me and my friends safe. If I don't follow these rules, I know that my teacher may stop me using technology at school and will talk to my parents about how I use technology.

Pupil's name:
Pupil's signature:
Date:

Parent's name:
Parent's signature:
Date:

KS2 E-safety Acceptable Use Agreement

• I will normally only use the school's ICT equipment and tools (including computers, cameras, Starz etc.) for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.

• I will only use the Internet if a teacher or teaching assistant is in the room with me.

• I will only delete my own files, and will not delete someone else's unless given permission by my teacher. I will not look at other people's files without their permission.

• I will keep my passwords private and tell an adult if I think someone else knows them. I know that my teacher can change my Starz password if needed.

• I will only open e-mail attachments from people who I know or someone who an adult has approved. If I am unsure about an attachment or e-mail, I will ask an adult for help.

• I will not give, without permission from a responsible adult, my own personal details such as surname, phone number or home address or any other personal details that could be used to identify me, my friends or my family. If I have to use an online name I will make one up!

• I will never post photographs or video clips of people I know without their permission and never include names with photographs or videos.

• I will never arrange to meet someone I have only ever previously met online. It could be dangerous.

• I will not deliberately look for, save or send anything that could be unpleasant or upsetting. If I find anything via Internet, e-mail or mobile phone that is upsetting or makes me feel uncomfortable, I will tell a teacher or another responsible adult.

• I will do my best to follow these rules both at school and at home because I know they are there to keep me and my friends safe. I will also do my best to remind others to follow these rules. If I don't follow these rules, my teacher may:

- Speak to me about my behaviour.
- Speak to my parents about my use of technology.
- Remove me from Starz communities or groups.
- Turn off my Starz account for a little while, or permanently.
- Not allow me to use laptops / computers to access the internet or particular programmes.
- Take other action to keep me (and others) safe.

Pupil's name: Pupil's signature:
Date:
Parent's name: Parent's signature:
Date:

Appendix D

Use of Mobile Phones in School Policy

Swaffham Bulbeck Church of England Primary School is committed to ensuring the safety of children in its care. We recognise the importance of mobile phones in school for communication purposes, but are aware that casual or inappropriate use of mobile phones in the school could pose a risk to children and adults.

It is recognised that it is the enhanced functions of many mobile phones that cause the most concern, and which are most susceptible to misuse. Misuse includes the taking and distribution of indecent images, exploitation and bullying. It is also recognised that mobile phones can cause an unnecessary distraction during the working day and can be intrusive when used in the company of others.

When mobiles phones are misused it can impact on an individual's dignity, privacy and right to confidentiality. Such concerns are not exclusive to children and young people; hence there is a duty to protect the needs and vulnerabilities of all.

It is appreciated that it can be very difficult to detect when such devices are present or being used, particularly in relation to enhanced functions, such as cameras. The use of all mobile phones is therefore limited, regardless of their capabilities. The aim is to avoid distraction and disruption of the working day, and to minimise the opportunities for any individual to make any covert images or misuse functions in any other way.

This policy applies to all staff, volunteers and visitors.

Please note that for the purposes of this policy, the term 'mobile phone' also covers any electronic device with the capacity to be used as a form of communication, either through the device itself or any applications stored on the device.

Staff Personal Mobile Phones

•Staff will not carry personal mobile phones while working. This protects staff from being distracted from their work and from allegations of inappropriate use. Phones must be safely stored out of sight of children and should be on silent so that they cannot be heard by children. They should be stored in staff lockers/ in the staff room/cupboards/in a box on the top shelf/desk drawer in the Tower.

• If staff have a break time during their working hours, they may use their mobile phones during these times, but this must not be in an area where children are present.

• In an emergency, staff needing to make a personal call during a lesson or whilst on duty should first obtain agreement from the Headteacher to ensure that adequate cover has been put in place and make the call in an area not used by children.

• Staff must give the school telephone number to their next of kin in case it is necessary for the staff member to be contacted, in an emergency, during school working hours.

• A personal mobile phone may be taken on school journey outings in accordance with guidance – see 'The Use of Mobile Phones on School Trips' section below.

• Pupil's personal data must not be stored on personal devices and these must also not be used to take or store images of pupils.

• Camera or video functions on personal mobile phones must not be used in the school by staff to take images of children under any circumstances.

• Staff should not be required to make work calls on their own phones, either mobile or landline, however if this should be necessary then they are advised to use the prefix 141 before dialling the recipients number to ensure their own number is protected.

• Failure by staff to comply with the mobile phone policy guidelines could result in disciplinary action.

Children

• The school recognises that children who walk to and from school without an accompanying adult may carry a mobile phone for safety. In these cases, children may bring a mobile phone onto the school premises but must deposit it with the school office at the start of the day and collect it from the office at the end of the day.

• Parents should be aware that whilst there are obvious benefits to pupils having a mobile phone in terms of personal safety there are also some associated risks such as potential for theft, bullying and inappropriate contact, including grooming by unsuitable persons.

• We would also like to alert parents/carers to the risks that using a mobile phone has while walking to and from school. Children who are concentrating on using their phone can have reduced general safety awareness which may result in road accidents and/or injury if a child is not paying attention to their surroundings.

• Mobile phones deposited in the office by children will be kept safely in a locked cabinet. Whilst the school will take every reasonable care, it accepts no responsibility whatsoever for theft, loss, damage or health effects (potential or actual) relating to mobile phones. It is the responsibility of parents to ensure mobile phones are properly insured. It is recommended that pupil's phones are security marked and password protected.

• Children are not allowed to bring mobile phones into any other areas of the school.

• Any mobile phones discovered to have been brought into the school and not handed in to the office will be confiscated immediately. Parents will be asked to collect the mobile phone from the school office.

• Children are not allowed to carry mobile phones on any school trips or extra-curricular events.

• If a member of the staff has any suspicion that a mobile phone brought into school by a pupil has unsuitable material stored on it, the pupil will be required to hand over the phone immediately to a member of staff and parents will be asked to collect it from the Headteacher. In circumstances where there is a suspicion that the material on the mobile phone may provide evidence relating to a criminal offence the phone will be handed over to the Headteacher for further investigation and the parent/carer asked to collect it from them.

Visitors and Parents/Carers

• The school displays a visitor's code of conduct advising visitors and parents/carers that mobile phones are not to be used in all necessary areas. This includes all uses including phone calls, texting and photographing. If a visitor or parent/carer is seen using their mobile phone, they will be asked politely to turn it off/desist from using it/remove it from children's view.

• It is recognised that many parents/carers use their mobile phone as a camera/video device to record their child at special events, special performances in school e.g. class assemblies, concerts, etc. On these occasions the use of a phone will be permitted for photographing/videoing only; a member of staff will always remind parents/carers before a performance that images should only be taken if they include their own child and that the use of these images is for their own personal use and must not be uploaded for any internet use including Facebook or any other social networking sites or used in any form of publication unless they are solely of their own child.

• The school recognises that children may inadvertently be included in photographs by another parent; the school, therefore, is obliged to warn parents of the legal and safeguarding risks of publishing such photographs on any platform. The placing of any photographs of children on social media is dangerous and parents may be in breach of the Data Protection Act if they upload photos of other children without the explicit consent of that child's parents.

The Office Mobile Phone

• This phone is for emergency use in the office should the main telephone line be out of action.

• It is the responsibility of the office staff to ensure that this phone is kept fully charged and in credit.

• This phone must not be used for taking photographs or videoing at any time.

• This phone may be used on school trips by the party leader – see guidance below re 'The Use of Mobile Phones on School Trips'

• It is the responsibility of the party leader to notify the office in advance that the phone will be required.

• Personal calls are not permitted to be made on this phone, other than in agreed exceptional circumstances. Contact or calls can be made via the office mobile in the event of an emergency.

• If any member of staff is required to drive in a working capacity, and has responsibility for the office mobile phone, the phone must be switched off whilst driving.

The Use of Mobile Phones on School Trips

The school recognises that the use of mobile phones on school trips can be beneficial in ensuring safety for all members of the school party. However, it is important that the following guidance is adhered to in order to keep children safe and protect staff and volunteers from accusations of inappropriate use:

The party leader should carry the office mobile phone for use in contacting other staff members or volunteers on the trip, contacting the school or contacting the emergency services. If the office mobile phone is unavailable (e.g. if another trip is on the same day) then the party leader should follow the advice below for staff use of personal mobile phones.

• Members of staff and volunteers may carry their own, personal mobile phones within the following guidelines:

• Personal phones should only be used to contact staff members or volunteers on the trip, the school or emergency services. If possible these calls should be made away from pupils.

• Personal phones should not be used for any purpose other than school business for the duration of a day trip. This means that personal calls or texts should not be made or accepted. On residential trips this will apply while the member of staff or volunteer is on duty. Staff and volunteers should ensure that next of kin are provided with the school number so that in an emergency the school is contacted and will make contact with the relevant person through the party leader.

• If it becomes necessary for a member of staff or volunteer to make a personal call or text, then the party leader or another member of staff should be informed and take responsibility for the pupils in the group while the call or text is made away from sight and sound of any pupils.

• Mobile phones must not be used under any circumstances to take photographs or videos of pupils. Volunteers are acting as staff members for the duration of the trip and therefore must not take photos or videos of any pupils, including their own child, using a mobile phone or any other mobile device, e.g. cameras or ipads, without the express permission of the party leader. Volunteers may be asked to take photographs of their group using a school camera – this must be passed back to the party leader at the end of the trip.

• The party leader may ask volunteers to provide them with their mobile phone number for the duration of the trip so that they can be contacted in case of emergency. The party leader undertakes to ensure that these numbers or not held on any mobile device or in any written form after the end of the trip.

• It is advised that if the party leader is using his/her own mobile phone, then if they need to contact anyone during the trip they do so by pre-dialling 141 (some mobile providers use a different prefix – staff are advised to check this with their provider) before the number so that their own number remains protected.

Use of mobile phones - guidance for volunteers on school trips

Thank you for volunteering to help on our school trip. During the trip you are acting as a member of staff with regard to the safety and well-being of the children in your group and we therefore ask that you follow the guidelines below in accordance with the school's mobile phone policy.

• Personal phones should only be used to contact staff members or volunteers on the trip, the school or emergency services. If possible these calls should be made away from pupils.

• Personal phones must not be used for any purpose other than school business for the duration of a day trip. On residential trips this will apply while the member of staff or volunteer is on duty. This means that personal calls or texts must not be made or accepted. Staff and volunteers should ensure that next of kin are provided with the school number so that in an emergency the school is contacted and will make contact with the relevant person through the party leader.

• If it becomes necessary for a member of staff or volunteer to make a personal call, then the party leader or another member of staff should be informed and take responsibility for the pupils in the group while the call or text is made away from sight and sound of any pupils.

• Mobile phones must not be used under any circumstances to take photographs or videos of pupils. Volunteers are acting as staff members for the duration of the trip and therefore must not take photos or videos of any pupils, including their own child, using a mobile phone or any other mobile device, e.g. cameras or ipads, without the express permission of the party leader. Volunteers may be asked to take photographs of their group using a school device – this must be passed back to the party leader at the end of the trip.

• The party leader may ask volunteers to provide them with their mobile phone number for the duration of the trip so that they can be contacted in case of emergency. The party leader undertakes to ensure that these numbers are not held on any mobile device or in any written form after the end of the trip.

If you have any questions regarding these guidelines please speak to the party leader. Thank you for your support and co-operation to ensure the safety of all the pupils.

Date	February 2017
Ratified by personnel	Feb 2017
Review Date	Feb 2020