Brooke Church of England Voluntary Controlled Primary School

E-safety Policy and Acceptable Use Contracts

Updated Dec 2016

Signed by Governors

To be reviewed Dec 2017

School e-safety policy

Section 1: Writing and reviewing the e-safety policy

The school e-Safety coordinator is the headteacher, Mr David Robinson.

Our e-Safety Policy has been written by the school, building on the Norfolk e-Safety Policy and government guidance. It is to be agreed by the head teacher, e-safety coordinator and approved by governors.

The e-Safety Policy and its implementation will be reviewed annually.

Section 2: Teaching and learning

2.1 Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Most households have internet access, meaning the internet provides a valuable tool for continuing and supporting learning at home.

2.2 Internet use will enhance learning

The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

2.3 Pupils will be taught how to evaluate internet content

Schools should ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Section 3: Managing internet access

3.1 Information systems security

School ICT systems capacity and security will be reviewed regularly in accordance with Becta Framework for IT Support (FITS).
Malware protection will be installed and updated regularly.
Security strategies will be discussed with the Local Authority.
Portable media brought into school by children may not be used without express permission followed by a virus scan. Adults such remain vigilant when using their own portable media.

3.2 Email

Pupils may only use email accounts provided by the school.
Pupils must immediately tell a member of staff if they receive offensive email.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
Pupils should not reveal usernames and passwords.
E-mail sent to an external organisation should be written carefully and authorised before sending.
The forwarding of chain emails is not permitted.
Email subscriptions to websites or other electronic services must be authorised by a member of staff.

3.3 Published content and the school website

The contact details on the school's websites should be the school address, telephone number and email address.
The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing images of pupils and their work

Photographs that include pupils will be selected carefully and will not enable pupils to be clearly identified.
Pupils' full names will not be used anywhere on the school's websites.

3.5 Social networking and personal publishing

The LA will block or filter access to inappropriate social networking sites.
Pupils will be advised never to give out personal details of any kind which may identify them or their location.
Staff must not communicate with pupils through social networking sites. Attempts by past or present pupils to engage in such communication should be ignored and followed up verbally where appropriate.
Where staff maintain blogs outside school, pupil involvement should be discouraged except when express permission has been given by the head teacher, in which case communication with pupils should be transparent and pertinent to teaching and learning.
Staff should not communicate with parents using social networking sites without the express permission of the head teacher.
Pupils must not place personal photographs on any social networking site using school property. Parents of pupils will be advised of the dangers associated with social networking sites.

Pupils will be advised on security, setting strong passwords, denying access to unknown individuals and blocking unwanted communications. They will be encouraged to invite known friends only and deny access to others.

3.6 Managing filtering

The school will work in partnership with the LA and E-Safety Group to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the e-safety coordinator or head teacher, who will inform ICT Solutions.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7 Managing videoconferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the internet.

Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the pupils' age.

3.8 Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones may not be used in school. Older children may bring them in for contacting parents after school, but they should remain in their bags until they are off the premises.

Staff will be issued with a school phone where contact with pupils is required.

When taking children off the premises, staff must take a mobile phone with them for emergencies.

3.9 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Section 4: Policy decisions

4.1 Authorising internet access

All staff must read and sign the 'Staff Code of Conduct' before using any school ICT resource.
The school will maintain a record of all staff and pupils who are granted access to school ICT systems.

4.2 Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor
NCC can accept liability for the material accessed, or any consequences of Internet access.
The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is effective.

4.3 Handling e-safety complaints

Complaints of internet misuse will be dealt with by the head teacher.
Any complaint about staff misuse must be referred to the headteacher.
Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
Pupils and parents will be informed of the complaints procedure.

Section 5: Communications

5.1 Introducing the e-safety policy to pupils

e-safety rules will be posted in all networked rooms used by children.
Users will be informed that in addition to adult supervision, ICT use will be monitored remotely.

5.2 Staff and the e-safety policy

All staff will be given the school e-safety policy and its importance explained.
Staff should be aware that internet traffic can be monitored and traced

5.3 Enlisting parents' support

Parents' attention will be drawn to the school e-safety policy in newsletters, the school brochure and on the school website.
The school, through the e-safety coordinator, will seek to assist parents with e-safety advice at home.

Please feel free to take pictures and video, but do remember that everyone has a right to privacy too. In your pictures, will be other children, whose parents may not want their children to appear on the internet. Take the pictures you want, for your family, but make sure they are only for your family. Please do not post images or video on any site such as facebook or you-tube; help us respect everyone's automatic rights to privacy.

Appendix 1

Staff code of conduct for ICT use

To ensure members of staff are fully aware of their professional responsibilities when using ICT equipment, they are asked to sign this code of conduct. Members of staff must read and understand the school's e-safety policy prior to signing.

1. I understand that the school ICT equipment and systems are the property of the school whether used on or off the premises.
2. I understand that it is a disciplinary offence to use any school ICT equipment or system for a purpose which contravenes the e-safety policy.
3. I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email and social networking. ICT use may also include personal ICT devices with the permission of the head teacher if used for school business.
4. I understand that my use of the internet and email, while at school, is monitored and recorded to ensure security compliance.
5. I will respect system security and I will not disclose or share any password or security information to anyone other than an authorised system manager.
6. I will ensure confidential data is stored securely and take all reasonable precautions to prevent its theft or loss.
7. I will report any incidents of concern regarding the inappropriate use of ICT equipment or systems to the e-safety coordinator or the head teacher.
8. I will ensure that all electronic communications I make are compatible with my professional role, be that in school or out of school.

The school may exercise its right to monitor the use of the schools ICT equipment and systems, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's facilities may be taking place, or where the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the staff code of conduct for ICT.

Signed:

Print name:

Date:

Appendix 2

Brooke VC C of E Primary School
E-Safety – Foundation & Key Stage 1

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Policy (AUP), with this agreement form relating specifically to children in Key stage 1 (Foundation, Year 1 and Year 2). An AUP is a written agreement, signed by pupils, their parents/guardians and teachers, outlining the terms and conditions of communication technology use.

The Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Please complete the sections below to show that you have read, discussed, understood and agree to the rules included in the Acceptable Use Agreement.

If you do not sign and return this agreement, access will not be granted to school ICT systems.

I agree that I will:

- Always keep my passwords a secret
- Only open pages which my teacher has said are OK
- Tell my teacher if anything makes me feel scared or uncomfortable
- Make sure that if I have to send messages, that they are always polite
- Show my teacher if I get a nasty message and I understand that I must not reply to it
- If I have to send an email, then it should be as directed by my teacher and using the school email service
- Talk to my teacher before using anything on the internet
- Not tell people about myself online (I will not tell them my name, anything about my
- home and family and pets)

- Not load photographs of myself onto the computer
- Never agree to meet a stranger

Anything I do on the computer may be seen by someone else

I have discussed the above read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, Virtual Learning Environment, website etc.

Name of Pupil:……

Class: ……

Parent / Carers Name: ……

Parent / Carer Signature: ……

Date: ……

Reviewed Dec 2016

Appendix 3

Brooke VC C of E Primary School
E-Safety - Key Stage 2

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Policy, with this agreement form relating to children in Key stage 2 (Year 3 to Year 6). An Acceptable Use Policy is a written agreement, signed by pupils, their parents/guardians and teachers, outlining the terms and conditions of communication technology use.

The Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Please complete the sections below to show that you have read, discussed, understood and agree to the rules included in the Acceptable Use Agreement.

If you do not sign and return this agreement, access will not be granted to school ICT systems.

When I am using the computer or other technologies, I want to feel safe all the time.
I agree that I will:

- always keep my passwords a secret
- only visit sites which are appropriate to my work at the time
- only work together with friends and I will deny access to others
- tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- make sure all messages I send are respectful
- show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable and realise that I should not reply
- not give my mobile phone number to anyone who is not a friend
- only email people I know or those approved by a responsible adult

- in school, only use email which has been provided
- talk to a responsible adult before joining chat rooms or networking sites
- always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult and my parents before I show photographs of myself
- never meet an online friend without taking a responsible adult that I know with me
- remember that anything I do on the computer may be seen by someone else

I have discussed the above read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, Virtual Learning Environments, website etc.

Name of pupil: ……

Class/Year: ……

Pupil Signature: ……

Date: ……

Parent / Carers Name: ……

Parent / Carer Signature: ……

Date : ……

Reviewed Dec 2016