Brooklands Primary School
Online Safety Policy

1. Writing and reviewing the online safety policy

The online safety policy links to other school policies including:

- The Anti-Bullying Policy
- PSHE Policy
- Safeguarding Policy
- Acceptable Use Policy for Staff and Pupil ICT Code of Conduct.

Our Online Safety Policy has been written by the Online Safety Leader, in conjunction with advice from Derbyshire County Council and government guidance. It has been agreed by the Senior Leadership Team, staff and approved by the Governing Body.

The online safety policy and its implementation will be reviewed annually.

2. Teaching and Learning

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.

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.

Class teachers will monitor pupils work when using internet derived materials and ensure their use complies with copyright law.

Senior Leaders will ensure letters to parents, information on the school website and social media pages using internet materials, also complies with copyright law.

3. Roles and Responsibilities from Brooklands Primary

The Head Teacher carries out the following responsibilities:

- Ensuring staff's access to ICT.
- Meeting statutory requirements.
- Health and Safety policy and practice.
- Ensuring the effective use of ICT for management and administration purposes.
- Compliance with Data Protection.

The Online Safety Leader carries out the following responsibilities:

- Ensuring the consistent implementation of Online Safety Policy.
- Identifying what Online Safety support is needed.
- Ensuring Online Safety requirements are on the school website.
- Provide information to staff about Online Safety & changes.
- Inform parents of how to keep children safe at home.
- Implementing and monitoring the Online Safety Policy.

The IT Technician carries out the following responsibilities:

- Ensuring inappropriate websites are blocked.
- Managing the IT system.
- Maintaining the server by approving updates, checking the anti-virus, and checking backup.
- Managing email and domain accounts.

The following responsibilities are carried out by all class teachers:

- Ensuring equal access to all strands of the ICT curriculum.
- Ensuring that pupils use ICT appropriately across the curriculum.
- Ensuring that pupils take care of IT equipment.
- To agree to the Staff Online Safety Agreement.

Pupils of Brooklands Primary School are expected to:

- Take an active role in lessons and activities to support their understanding and confidence when dealing with online safety issues.
- They are asked to agree to the Pupil ICT Code of Conduct when using technology in school.

Governors are expected to:

- Be responsible for overseeing and reviewing the Online Safety Policy.

4. Managing Internet Access

Information System Security

The school uses the standard LA Internet Service Provider which is KCOM.

Our broadband connection of 10MB is provided by CAPITA.

School ICT systems capacity and security will be reviewed regularly.

The school subscribes to AVG Anti-virus software which is monitored and updated regularly by the ICT Technician. Any software messages or pop ups reporting of viral infections should be reported immediately to the ICT technician.

Security strategies will be discussed with Derbyshire County Council.

Computer Password Security
Brooklands Primary School is responsible for ensuring that the school computer network is as safe and secure as possible and that:

- Users can only access data to which they have the right to access.
- No unauthorised users can access GPM protected folders.
- Sensitive data should be contained in a GPM protected document
- Access to personal data is securely controlled in line with the School's Personal Data policy.
- Staff are advised to lock computers when not in the room.
- Staff memory sticks are encrypted to ensure others' cannot access confidential information.

Internet enabled mobile phones and Technology
We acknowledge that some of our older pupils have SMART phones/IPads and whilst we acknowledge there are advantages to them we ask that pupils leave them at home. Parents may request the school office stores mobile phones in circumstances that pupils may need them on their journey to and from school.

Published content and the school website
The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will **not** be published.

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work
Photographs that include pupils will be selected carefully so that individual pupils' photos cannot be misused. Considering using group photographs rather than full-face photographs of individual children is recommended.

Written permission from parents or carers will be obtained before photographs are published on the website and social media accounts.

Pupils' full names will not be used anywhere on the Brooklands Primary School Website, Twitter or Facebook accounts.

Parents should be clearly informed about image taking on the school grounds and will be asked to not post any photographs on social media pages.

School networking and personal publishing
The school will block/filter access to social networking sites except in the main office for the purpose of updating school Facebook & Twitter pages.

Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised to never give out personal details of any kind, which may identify them or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Social Networking for staff in a personal capacity
It is possible that a high proportion of staff will have their own social networking accounts. It is important for staff to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.
Guidelines for staff:

- Staff must never add pupils as friends to their personal accounts.
- Staff must not post pictures of school events without the Head Teacher's consent.
- Staff must not use social networking sites during lesson times.
- Staff need to use social networking in a way that does not conflict with the National Teacher Standards.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Staff must not post negative comments about the school, pupils, parents, colleagues or governors.
- Inappropriate use by staff should be referred to the Head teacher.

Cyber-bullying
Cyber-bullying involves the use of information and communication technologies with the intent to harm others. This can take a wide range of forms including email, text, instant messaging and comments left on blogs/forums etc.

Children will be made aware of what cyber-bullying is, how to stay safe online and how to report any incidents regularly during ICT lessons involving the internet, during anti-bullying week and during PSHE/circle time activities.

Any incidents of cyber-bullying will be reported to the Online Safety Leader, Safeguarding Co-Ordinator and Senior Management. Complaints of cyber-bullying will be dealt with in accordance with the anti-bullying policy. Complaints related to child protection will be dealt with in accordance with school child protection procedures.

Managing filtering
The school will work with the LA, DfE, RM filtering and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. Filtering for all pupils is set to the highest level.

Hector the Protector will be visible (as a dolphin) on all school computers to ensure if content is accessed that a pupil is unsure of they can press Hector to remove it from their screen. This will allow the class teacher to be notified and the information passed on to the Online – Safety Leader and Senior Leaders. Pupils' will be regularly reminded about Hector and referred back to the ICT Code of Conduct.

Despite the best efforts of the LA and school staff, occasionally pupils may come across something on the internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur so that action can be taken.
The actions will include:

1. Making a note of the website and any other websites linked to it.
2. Informing the ICT Technician.
3. Logging the incident (book to be kept in the office in the IT Technician's workspace)
4. Discussing the incident with pupils/staff to prevent similar experiences in the future.

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.

The use of portable media such as memory sticks and portable hard drives will be monitored closely as potential sources of computer virus and inappropriate material.

Pupils are asked not to bring mobile phones, Ipads or any other ICT devices into school. If a staff member is aware of a child with a phone in school, please ask the child to hand it in until the end of the day. It is also essential that the child's parents are aware of our policy and advised not to let their child have a mobile phone in school in future.

Staff will use a school phone where contact with pupils is required. During off-site visits it may be essential to contact parents/carers direct from a staff mobile in emergency cases.

Staff should not use personal mobile phones during designated teaching sessions.

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

5. Policy Decisions

Authorising Internet access
Pupils will be given instructions before accessing the internet and all pupils must sign up to the Pupil ICT Code of Conduct to abide by the school's Online Safety rules. Access to the Internet will be by directly supervised by staff and pupils will only access specific and approved online materials.

These Online Safety rules will also be displayed clearly in all networked rooms.

All parents will be asked to sign the Parent Acceptable Use Agreement giving consent for their child to use the Internet in school by following the school's Online Safety rules and within the constraints detailed in the school's Online-Safety policy.

All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Assessing risks
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor DCC can accept liability for the material accessed, or any consequences of Internet access.

The school will regularly check ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

Handling Online Safety Complaints
Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the Online Safety Coordinator. All incidents will be recorded in an Online Safety incident logbook (book to be kept in the office in the IT Technician's workspace)

Any complaint about staff misuse must be referred to the Head Teacher.

Complaints of a child protection nature must be dealt with in accordance with school safeguarding policy and passed on to the Designated Safeguarding Lead. Additionally, any complaints reported from outside school will also be dealt with in accordance with the safeguarding policy.

Pupils and parents will be informed of the complaints procedure.

6. Communications Policy

Introducing the Online Safety policy to pupils
The Pupil ICT Code of Conduct will be displayed in all classrooms and the ICT suites and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PSHE lessons/circle times/anti-bullying week.

Pupils will be informed that network and Internet use will be monitored**.**

Staff and the Online Safety policy
All staff will be given the School Online Safety policy and its importance explained.

All staff will agree to the Staff Online Safety Agreement and asked to sign it on a yearly basis.

Any information downloaded must be respectful of copyright, property rights and privacy.

Staff should be aware that Internet traffic can be monitored and traced to the individual user.

Discretion and professional conduct is essential.

A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software.

Enlisting parents' support
Parents' attention will be drawn to the School Online Safety policy via the school website, Parent Acceptable Use Agreement giving consent for Pupils to use school ICT equipment, newsletters and a yearly Online Safety workshop.

Parents and carers will be made aware of their responsibilities regarding their use of social networking.

Parents are expected to not post any pictures of their child or any other pupils taken in the school grounds. If they do and it comes to our attention, they will be asked to remove it straight away.

Parents should make complaints through official school channels rather than posting them on social networking sites.

Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

7. Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the Online Safety Leader. This policy is the Governors responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the Online Safety Leader, Computing Co-ordinator, Designated Safeguarding Lead and Governor with responsibility for Safeguarding. Ongoing incidents will be reported to the full governing body.

The Online Safety policy will be revised by the Online Safety Co-ordinator.

Date implemented: May 2016
Date for review: May 2017

Signed: …… (Head teacher)
Approved by the Governing Body of Brooklands Primary School.
Signed: …… (Chair of Governors)
Date:

Appendix 1: Internet use – Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids, CBBC Sear, Kidsclick.
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should use only approved e-mail accounts. Pupils should never give out personal information.	ePals Super Clubs PLUS email a children's author email Museums and Galleries
Publishing pupils work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' first names should only be used.	Making the News Super Clubs Infomapper Headline History Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Brooklands Primary School website School Facebook/Twitter accounts
Audio and video conferencing to gather information and share pupils work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype Global Leap