# BRUNSWICK PARK PRIMARY SCHOOL


# COMPUTING POLICY
# Incorporating Online Safety and Acceptable Use of the Internet Policies

**Date drafted: October 2015**

**Drafted by: Michael Williams, Victoria Perry and Khay Islam**
**Agreed by Governing Body: October 2015; revised November 2016**

**Review Date: July 2017**

This policy should be read in conjunction with other school policies including Anti-Bullying, Behaviour, PSHCE, Safeguarding and Data Protection.

**Introduction**

This policy aims to cover the different elements of ICT and Computing at Brunswick Park Primary School. Guidelines have been drawn up to ensure that all stakeholders are aware of their expectations and are able to stay safe when using the hardware and software in school. The equipment and resources within school are provided to enhance pupils' learning and to aid staff in their teaching of the curriculum. This policy sets out a framework for how Computing will be taught, assessed and monitored throughout the school and should reflect the school's ethos and philosophy. There is one policy at Brunswick Park that covers ICT and Computing, including Online Safety (e-safety) Acceptable Use and use of Social Media.

**Aims/Rationale**

Computing is part of almost every part of modern life and it is important that our children are taught how to use its tools safely. We believe that it is important for pupils, staff and the wider school community to have the confidence and ability to use Computing's tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent, independent users and learners of Computing we aim:

- To use Computing where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
- To use Computing to help improve standards in all subjects across the curriculum
- To develop the Computing competence and skills of pupils through Computing lessons and provide them with the chance to consolidate these in a cross-curricular context
- To ensure pupils are challenged in their use of Computing and are provided with exciting, creative ways in which to share their learning
- To use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation
- To provide all staff with the training and support to ensure that they can, and have the confidence to, use Computing to its full potential in all aspects of school life
- To use Computing as a form of communication with parents, pupils and the wider community.

**Curriculum**

Computing is taught across the curriculum and wherever possible, is integrated into other subjects. Each class from Years 1-6 has a weekly stand-alone session during which the Scheme of Work *Switched on Computing* (Rising Stars) is used to provide a comprehensive programme for the teaching and assessment of Computing across Key Stages 1 and 2. All activities are mapped/linked to the new National Curriculum for Computing. Teachers adapt *Switched on Computing* units to meet the needs of their children.

In the EYFS, children are taught how to use various pieces of Computing equipment, including computers, in accordance with the EYFS Curriculum.

**Assessment**

Computing is assessed in a number of ways using formative and summative assessment. Formative assessment is ongoing during Computing lessons and is used to inform future planning. Summative assessment takes place at the end of each unit of learning; pupils complete an end of unit assessment using *Switched on Computing* to assess progress within the unit. When completed, assessments are stored in pupils' portfolios.

**Equal Opportunities and Inclusion**

All pupils throughout the school are provided with opportunities to access the Computing curriculum at an appropriate level. Where necessary, we will endeavour to make adaptations to the environment or provide software that will enable all learners to achieve. iPads are used to enable pupils to access the broad curriculum. *Communicate in Print* is available for all to use to create visual communication resources.

## Roles and Responsibilities

**Senior Leadership Team**

- Is responsible for monitoring the teaching of Computing throughout the school
- Provide and allocate resources throughout the school in accordance with the School Improvement Plan, Computing Subject Leader action plans and timescales
- Ensures that the Computing Subject Leader(s), Computing Technician and teachers fulfil their roles as listed below and in accordance with job descriptions and appraisal objectives.

**Computing Subject Leaders**

- Oversee planning and assessment in all Year Groups and are responsible for raising standards in Computing
- Inform staff of new developments and initiatives and provide training
- In conjunction with the Computing Technician and SLT are responsible for strategic planning and guidance for future purchasing.

**Computing Technician**

- Is responsible for keeping an up to date hardware inventory and ensuring the school has the appropriate number, and level, of software licenses for all software
- Is responsible for managing equipment and providing guidance for future purchasing of hardware
- Is responsible for purchasing and ordering hardware and software for the school, liaising with the above
- Updates logins, usernames etc. for all staff and pupils
- Ensures faults logged in the Computing fault log are rectified in a timely manner.

**Teachers**

- Plan and teach Computing and link it where possible/appropriate with other subjects
- Plan, teach and assess Computing using the *Switched on Computing* units
- Respond and report any Online Safety issues, including cyber-bullying, to a member of the Safeguarding Team (Fiona O'Malley, Karen Smith, Susannah Bellingham and Andrea Inniss-

Griffith) or the designated Online Safety Officer, Fiona O'Malley in accordance to Online Safety procedures as listed below in the policy

- Whilst checking of personal sites, e.g. email, is permitted during non-directed times, teachers should be aware that this should only happen briefly and that they should be extra vigilant, ensuring they are logged off appropriately (of both the website and their computer)
- Must agree to and follow the Acceptable Usage Policy (within this policy).

**Support Staff**

- Respond and report any Online Safety issues, including cyber-bullying, to a member of the Safeguarding Team (Fiona O'Malley, Karen Smith, Susannah Bellingham and Andrea Inniss-Griffith) or the designated Online Safety Officer, Fiona O'Malley in accordance to Online Safety procedures as listed below in the policy
- Whilst checking of personal sites, e.g. email, is permitted during non-directed times, teachers should be aware that this should only happen briefly and that they should be extra vigilant, ensuring they are logged off appropriately (of both the website and their computer)
- Must agree to and follow the Acceptable Usage Policy (within this policy).

**Visitors**

- School visitors should abide by the guidelines set out for staff and ensure that they use ICT equipment safely.

**The School**

We aim to ensure that parents, carers and pupils are fully aware of ways in which the internet and Computing can be used productively and safely. We will always ensure that we provide children with opportunities to achieve when using ICT and will ensure our curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the children's safety is our first consideration and will keep parents/carers informed as appropriate through newsletters and the website. Annual training for staff and information sessions for parents/carers and pupils will be delivered by Teresa Hughes, external Online Safety trainer. Online Safety is promoted through information leaflets and age appropriate Online Safety assemblies. Online Safety lessons will also be taught in conjunction with the *Switched on Computing* scheme of work. Online Safety is a focus during Anti-Bullying Week and there is a yearly Internet Safety Day.

**Pupils**

- Should ensure that they use computers and equipment appropriately at all times
- Should report any Online Safety or cyber bullying issues to either their teacher or an appropriate adult
- Follow the school's behaviour policy when working online
- Adhere to the school's anti-bullying policy when using technology
- Follow the SMART rules and guidelines that are displayed in every classroom, the Computing suite and around the school.

**Parents and Carers**

- Should remain vigilant regarding software, internet content and websites their children access
- Use the Online Safety Leaflet provided by the school
- Attend the Online Safety training provided by the school, including web links
- Encourage their children to follow the SMART rules which are provided on the back of the Online Safety Leaflet.

**Equipment, Hardware and Software**

Hardware should not be installed without the permission of the Head Teacher and Computing Subject Leader. If staff use memory sticks then the school's antivirus software will scan these. Staff should be vigilant to reduce the risks of virus infection as stated in the AUP. The installation of software unauthorised by the school, whether licensed or not, is forbidden. If staff are unsure, they must refer to the Head Teacher and/or the Computing Subject Leader. The school reserves the right to examine or delete any files held on its system. Teaching staff are given an iPad tablet for use at school and at home.

**Network**

Staff are issued with a username for the school computers. They also are issued with a password and it is their responsibility to maintain its security. Accounts are created and monitored by the Computing Technician.

Pupils are given usernames and a password. In Key Stage 1, pupils log in using a username which is simply the class name followed by a simple password. Pupils in Key Stage 2 log in with the initial of their first name followed by their last name, followed by a simple password for each child. Accounts are created and monitored by the Computing Technician.

When a new pupil/member of staff joins the school, it is the responsibility of Office Staff to inform the Computing Technician. The Computing Technician will then provide a network login. At the end of an employee's or pupil's time at the school, accounts will be deleted.

The school has a wireless network. The password for staff is available on request from the School Office. Staff may connect their own laptops/phones/tablets to this by liaising with the Computing Technician who will set this up for them, settings permitting, in accordance with the network guidelines.

**Backups**

Every school day the main server is set to backup essential files and settings onto a tape and to perform an offsite backup on LGFL Gridstore. In the event of a system failure, the Computing Technician is contacted as a matter of urgency. The school photograph folder and Teacher Resources are backed up to an external hard drive once per term and this is kept at the home of the Computing Subject Leader (Curriculum). For individual files or folders, these can be restored using a tool in Windows Server 2008 to recover previous versions.

**School Website and Whole School News**

The school website is maintained by Tony Cavallo (Frootes Media). The Computing Technician will support with updates as necessary. The Head Teacher and Office Staff ensure the website is updated regularly. All staff contributions should be sent to the Head Teacher in the first instance. A designated teacher from each year group is responsible for ensuring the Year Group's News is sent to the Head Teacher regularly for approval before being uploaded.

**Internet and E-mail**

The internet may be accessed by staff and by pupils at school. Staff must be vigilant about sites pupils access, and children should not use the internet unsupervised. Security Settings are set up in accordance with LA and LGFL Guidelines.

The teaching of email and internet use will be covered within Computing curriculum planning, and staff should encourage regular discussion that explores the benefits and potential dangers of using the internet. This will also be referred to during Online Safety Lessons and Assemblies.

All members of staff are issued with a school email address. This is the email address to use for professional communication. Staff should take extra care to ensure that all communication remains professional. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails to ensure it is not misconstrued. All web activity is monitored by the Computing Technician so it is the user's responsibility to ensure appropriate procedures for logging off are followed. Pupils are taught about inappropriate material. Pupils are taught to report content that they do not like or that makes them uncomfortable.

The use of the internet to access inappropriate content such as auction sites, pornography, racist or extremist material is prohibited. If any user sees an inappropriate website or image at school, they should close it immediately and report the site to the class teacher who will then refer it to the Online Safety Designated Officer (Fiona O'Malley) or the Safeguarding Team (Fiona O'Malley, Karen Smith, Susannah Bellingham and Andrea Inniss-Griffith). They will act in accordance with School Policy.

The internet and filtering is provided by the Local Authority and LGFL and is monitored by the Computing Technician. Inappropriate websites are filtered out. Additional sites can be enabled by the Computing Technician and a record is kept of these.

**Passwords**

Staff should make sure that any passwords they use are strong. They should be changed regularly, especially if the user suspects others may know them.

**Personal Data**

Staff should be aware that they should not transfer personal data such as reports, Provision Maps and contact information to personal devices unless strictly necessary. These data should then be removed as soon as possible. When using a personal laptop or device containing pupil data, staff should be vigilant to keep the device secure, e.g. not leave it lying around, on display or visible in a parked car.

**Social Media**

We recognise that social media and networking play an increasingly significant role within everyday life and that many staff are users of tools such as Facebook, Twitter and blogs both personally and professionally. We will ensure that staff and children are made aware of risks and concerns that may arise of how to minimise them.

Staff should:

- Ensure that their profile/posts have strong privacy settings; this also includes personal information such as phone numbers, email addresses etc.
- Not accept current or ex-pupils as 'friends' on social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand that some staff members have friends within the local community (such as children's parents) and just ask that these members of staff take extra precautions when posting online
- Ensure that if their communication is fully public (e.g. blogs/Twitter), that they maintain their professionalism at all times and remember that they are a representative of the school
- Be aware that electronic texts can sometimes be misinterpreted or misconstrued so should endeavour to minimise the possibility of this happening
- Not use these media to discuss confidential information or to discuss specific children
- Seek advice from the Computing Subject Leader if they need help when monitoring their online persona and checking their security settings.

Pupils should not be signed up to most social networking sites as their age limit is 13+. However, we recognise that many are signed up either with or without parental knowledge. At school we monitor the use of social networking and ensure it is part of our curriculum through lessons, assemblies and a school information leaflet that has links to suitable websites. We reserve the right to contact sites such as Facebook and ask them to remove pupils' accounts should any issues occur, such as cyber-bullying.

As a school we will use the website on which to post information and will update blog posts that will stream directly to our blog area, Whole School News. We will ensure that inappropriate comments are blocked.

The website is used to share children's learning and to communicate with parents and carers. We will follow guidance laid out in this document to ensure children are kept safe. No-one is able to post without it being approved by the Head Teacher to ensure that the children are not subjected to any inappropriate comments. Spam messages (often containing inappropriate links and language) are caught by software installed on the website and this is monitored by the Computing Technician. It is updated regularly.

Online Safety questionnaires are completed with pupils to monitor and evaluate Online Safety knowledge and procedures.

**Digital and Video Images**

We will ensure that if we publish images or videos of children online, that:

- Parents or guardians have given us written permission
- We will not include a child's image and his/her name together without permission from the parents or guardians e.g. if the child has won an award
- If we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out unnecessarily
- We will ensure that children are in appropriate dress and that we do not include images of children who are taking part in swimming activities
- Ask that if a parent, guardian or child wishes, they can request that a photograph is removed. This request can be made verbally or in writing to the child's teacher, to the Computing Subject Leader or to a member of the Senior Leadership Team. We will endeavour to remove the image as soon as possible
- We will provide new parents/carers with a photograph permission letter upon their arrival into school (this is part of the Admissions Process)
- We will ask parents or guardians who are recording video or taking digital images at public events e.g. school play or sports day, that they do not publish them online or share them on social media.

Only school cameras and hardware can be used to take photographs or videos within the school. These should be stored on the staff shared area in the appropriate place, and should be removed from the device as soon as possible.

**Technical Support**

- Minor Computing issues are dealt with by the Computing Subject Leaders.
- Additional hardware support is provided by Khay Islam (Computing Technician).
- Support for the website is provided Tony Cavallo (Frootes Media).
- Additional office-based technical support is provided by Wauton Samuel.

**Online Safety – Linked to 360Safe E-Safety Guidelines**

At Brunswick Park, we take Online Safety very seriously. We will ensure that it is taught in conjunction with the *Switched on Computing* SoW and PSHCE sessions as necessary. Children will be taught how to act online and how to minimise the risk when working on the internet. Pupils will also be taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them. They will also be taught the SMART rules for internet safety.

Curriculum plans provide children with an understanding of the expectations we have of them at a level appropriate to their age. We will also have termly Online Safety assemblies.
All children will be taught about the Acceptable Use Policy and will sign an age-appropriate copy that will be stored by the Computing Subject Leaders. All staff will sign an AUP. SMART rules will be displayed in visible areas of the school.

Online Safety training will be provided for staff regularly to keep up to date with current affairs and legislation.

If there is a website available to children that staff deem inappropriate, they should liaise with the Computing Subject Leaders who will report it to Southwark LA.

If a teacher suspects an Online Safety issue within school it should be noted in accordance with anti-bullying and behaviour policies. It should then be reported to the Computing Subject Leaders, Safeguarding Team and/or SLT and recorded as appropriate.

If children receive an email, message or view a site that is inappropriate then they should report this to their teacher who will then forward the matter on to the Computing Subject Leaders, Safeguarding Team and/or SLT who will who will investigate.

**Complaints**
Incidents regarding the misuse of the Internet by pupils will be delegated to the Computing Subject Leaders, Safeguarding Team and/or SLT who will decide which additional evidence should be gathered or recorded. A partnership approach with parents/carers will be encouraged. Any complaint about staff misuse will be referred to the Head Teacher. Complaints of a child protection or Safeguarding nature must be dealt with in accordance with Safeguarding and Child Protection procedures.

**Copyright and Intellectual Property Right (IPR)**
Copyright of materials should be respected. This includes when downloading material and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it.

Staff should check permission rights before using materials, particularly images, from the internet. Children will be taught in Key Stage 2 to begin to consider the use of images from the internet. In Years 3/4 they will discuss the proper use of images with questions such as, 'Is it appropriate to use an image we find online?' As they progress to Year 5/6, pupils should start to reference the sites they have used if deemed necessary by their teachers. This could be as simple as noting the name of the site from which the image came, or a hyperlink. It is not expected that children include a full reference, but to be *aware* that it is not acceptable to take images directly from the internet without some thought about their use.

All materials created by staff whilst in employment of the school belong to the school and should not be used for financial gain. This is in accordance with guidelines laid out by the Local Authority.

**Responding to unacceptable use by staff**
Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possible legal action.

**Responding to unacceptable use by pupils**
Pupils should be aware that all Online Safety issues will be dealt with quickly and efficiently. When dealing with unacceptable use, staff should follow the behaviour policy and if necessary, the anti-bullying policy. Children may have restrictions placed on their account for a short time.

**Acceptable Usage Policy – Staff – Linked to 360Safe AUP Guidelines**

## Staff

This document has been written to ensure that staff use ICT throughout the school appropriately. If they have any questions regarding this policy, they should direct them to the Senior Leadership Team or the Computing Subject Leaders. Staff should:

- Use computers and equipment with care and ensure children do the same, e.g. water bottles should stay away from machines
- Ensure that they have strong passwords
- Ensure that usernames and passwords are not shared with children or other staff
- Ensure that they log off when they have finished using a computer, particularly in shared areas
- Make use of resources such as cameras and microphones and ensure that these are returned after use. They should endeavour to remove pictures/files regularly from these resources
- Try not to be wasteful, in particular regarding batteries, printer ink and paper
- Ensure that online dialogue (e.g. blog posts or emails) with other schools, parents/carers and pupils remains professional at all times
- Ensure that online activity is related to their professional duties and that personal use should be kept to a minimum during the school day
- Ensure that they are not using the school's ICT for financial gain e.g. auction or betting sites
- Ensure that they have read and understood the Computing Policy
- Be aware that software and hardware should not be installed without the prior consent of the Computing Subject Leader or Head Teacher
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the Head Teacher
- Where data of a personal nature such as school reports, Provision Maps, correspondence, photographs and assessment data are taken home on a school laptop or other storage device, it must be recognised that these data come under the Data Protection Act and are subject to the school's Data Protection Policy. Care must therefore be taken to ensure their integrity and security. They must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical. Where staff are using their own digital equipment such as cameras and mobile phones, extreme caution is advised to avoid misinterpretation by others. Files should be transferred to school equipment as soon as possible
- Report any issues to the Senior Leadership Team or Computing Subject Leader as soon as possible
- Return any hardware or equipment on or before their contractual end date if they are no longer employed by the school.

Signed _____ Print _____

Date _____

**Acceptable Usage Policy for KS2 Pupils – Linked to 360Safe AUP Guidelines**

## Pupils: Key Stage 2

This document provides some guidelines to ensure that you stay safe and act responsibly when using ICT. When we talk about Computing and ICT, we are referring to computers, netbooks, and all other electronic devices including cameras and Smartphones. By using ICT in school, you have agreed to follow these rules. These rules will be discussed with you in your class before you sign them. A copy of them will also be sent home to your parents or carers.

If you have any questions, please ask your teacher.

- At all times, I will think before I click (especially when deleting or printing)
- When using the Internet, I will think about the websites I choose
- If I find a website or image that is inappropriate, I will tell my teacher straight away
- When using information or pictures from websites, I will try to say which website it came from and if possible will refer to it
- When communicating online (in blogs, email etc.) I will think carefully about the words I choose and will not use words that may offend other people
- When communicating online, I will only use my first name and will not share personal details such as my email address or phone number
- I understand that people online might not be who they say they are
- I will not look at other people's files or documents without their permission
- I will not log on using another person's account details without their permission
- I will think before deleting files
- I will think before I print
- I know that the teachers can, and will, check the files and websites I have used
- I will take care when using computers and transporting equipment around
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents, carers or teachers
- I will not install any software or hardware (including memory sticks) without permission from a teacher
- I understand that if I act inappropriately then my parents/carers will be informed

Signed (Pupil) _____

Class _____

Date _____

**Acceptable Usage Policy for KS1 Pupils – Linked to 360Safe AUP Guidelines**

## Pupils: Key Stage 1

These rules have been written to make sure that you stay safe when using computers and ICT equipment. These include cameras, netbooks, microphones and Beebots. By using the Computing equipment in school, you have agreed to follow these rules. Your teacher will talk about these rules before you sign them and a copy will be sent home to your parents/carers.
If you have any questions, please ask your teacher.

The Golden Rule: **Think before you click**

☺I will be careful when using the internet.
☺ I will only use the internet when a teacher is with me.
☺I will tell a teacher if I see something that upsets me.
☺I know people online might not be who they say they are.
☺I will be polite when talking to people or writing online.
☺I will think before I print or delete.
☺ I will be careful when using or carrying equipment.
☺I will keep my password secret, but I can tell my family.
☺I will remember to log off properly before closing my netbook lid.
☹I won't tell anyone any personal details like my phone number or last name.
☹I won't log on using someone else's username.
☹I will never put water bottles on the table when using computers.

Signed (Pupil) _____

Class _____

Date _____