**Bankfields Primary School**

**Policy for the safe use of ICT**

**September 2016**

**Who will write and review this policy?**

Our school Internet policy has been created by the ICT Subject Leader and the Head Teacher using information from Redcar and Cleveland Local Authority and government guidance. It has been discussed by the whole staff and approved by governors, who realise how the safe use of ICT is intrinsic to the running of the school, both at management level and an educational level. The policy will be reviewed annually by the ICT Subject Leader.

**What is the purpose of this policy?**

The Internet is the most data-rich source of information in the world. It can potentially “bring the world into the classroom”. From a teaching point of view, this is an essential resource for planning and delivering lessons. The Internet provides a valuable source of information for members of staff and the children. The school recognises the value of the Internet as a source for information for teaching and learning and as an excellent means of communicating quickly to a wide audience. At the same time, the Internet is largely unregulated and it must be used advisedly. It can be a source of security threats, and information available from it may not be reliable, up-to-date or accurate. It is to be used in a manner that is consistent with government guidance.

In addition to this, pupils will be given the opportunity to use a wide range of technology to achieve specific goals. The children may also be using the Internet to upload files that they have created. The Internet is a place to share information and the school would like to take advantage of this collaborative learning platform to enhance the curriculum. This policy seeks to ensure staff members know what good practice is and to outline steps and procedures that will be taken when protocols are not followed.

**Internet Safety**

**Filtering**

The school’s 10Mb broadband connection is provided by the Local Authority, which in turn links into the Northern Grid network and ultimately the National Education Network. The filters at each stage are extensive (Smoothwall) and include lists of illegal sites/inappropriate sites that cannot be accessed. It also allows open access and sharing of resources between educational establishments. This is updated and monitored by local authority staff. However, when dealing with the Internet there is never a failsafe way of blocking inappropriate content in all situations and therefore the school cannot take responsibility for these events when all reasonable steps outlined below have been taken. Use of the web through the LA link is monitored and traceable by the council network administrators. In addition to this, there is a consideration that children will inevitably access the Internet outside of school. We therefore aim to educate them about Internet safety, not simply to cover their eyes.

**When will pupils have direct access to the Internet?**

Children in all classes in school will have access to the Internet. However, the different types of use access are outlined below:

* Online content (e.g. researching a topic) will often be used by the teachers for specific tasks. In these situations the children are not searching the Internet or navigating away from the page/s and tasks that have been set. Teachers **will have previewed** the site to ensure that it matches the learning outcomes of the lesson/setting. Teachers must also ensure that video content is previewed prior to the lesson and that any automatic ‘auto-play’ features are disabled. When working with younger children it is essential that access to navigate away accidentally is denied (i.e., hiding the address bar).
* Searchable cached sites such as Espresso will allow access within a site but not beyond it. Please communicate to the children that advertisements and sister website hyperlinks may navigate the children away from the current website.
* Children will only navigate the Internet through the use of a safe-walled garden site such as Espresso or other approved platform when searching for information. Searches will only be permitted when a member of staff is present. Where possible, teachers should have pre-searched for the topic and previewed the hits that will be used based on the fact that search engines do not necessarily give the most appropriate site at the top of their lists. Techers should provide children with the correct search words to guide them to appropriate content, e.g. ‘plant life cycle’.
* When using iPads, some applications can potentially navigate children to the Internet through advertisements. Teachers should test any new applications before allowing the children to use them, and ensure children are aware of hyperlinks.

Children will not be allowed to access and search the Internet unless authorised by a member of staff. Responsibility for the monitoring of what the children find is then the responsibility of the adult. When use of searching on the Internet is appropriate can be found in the school Scheme of Work for ICT; other uses are the sole responsibility of the supervising adult. Appropriate behaviour and understanding of how addresses are composed will be explicitly taught before ever using an Internet search in school and will be reinforced by visual reminders. Adults must take a zero tolerance approach to any children purposefully exploring the Internet without supervision.

Accessing and interacting with the Internet is part and parcel of many users’ reasons for having an Internet connection. Simply blocking the children from using the Internet is not educating them for the real world (and use at home). Therefore Internet safety is implicitly taught throughout school and referred to whenever a unit of work requires use of the Internet. Key themes to be covered are listed below:

* Safe browsing on the Internet
* The use of social networking, email and e-communications
* Use of blogs/webspace and the impact of a digital footprint
* Copyright
* What to do when you come across something that is inappropriate
* How to procced if bullying/inappropriate communications are made

**Staff**

**Email**

Staff will be given a “professional” email account. The account is set up using Office 365. Staff members are at liberty to use their accounts for correspondence between one another or other professional bodies as part of their work. Passwords must be changed by the user. Users agree, through the staff agreement form, to keep passwords secret, even from their family and friends.

[www.outlook.com/bankfields.rac.sch.uk](http://www.outlook.com/bankfields.rac.sch.uk)

**Username**: [aperson@bankfields.rac.sch.uk](mailto:aperson@bankfields.rac.sch.uk)

**Password**: \*\*\*\*\*\*\*\*\*\*\*\*\*

Users will also be expected to report any offensive emails that they receive to a member of staff. Any intercepted emails or reports of offensive emails will be reported to the Head Teacher.

Users must also report any attempts by people who they don’t know trying to contact them.

Use of personal email accounts in school is not permitted.

Use of newsgroups or forums/chatrooms in school is not permitted.

The staff Internet agreement form sets out the terms and conditions that they must agree to before being allocated an account.

Failure to adhere to the agreement may result in suspension/blocking of the account.

**Mobile Devices**

The use of mobile phones by children is not permitted within school unless permission has been granted by the Head Teacher. Failure to observe this will result in confiscation. Staff must keep mobile phones switched off during lessons and formal meetings. They should not be accessible to children and are not allowed in classrooms. Private telephone calls should not be made or received in the presence of pupils. Personal mobile phones or cameras must not be used to take photographs in school. All class teachers are provided with a school laptop, therefore personal laptops should not be brought into school. Staff should remain vigilant for any inappropriate use of technology by pupils, both in school and out. Any concerns should be reported to the ICT subject leader and the Head Teacher.

**Social Networking and Professional Responsibility**

Staff must be aware of their professional standing and responsibilities at all times, particularly in relation to the use of modern technologies. Staff with social network accounts such as Facebook or Twitter must be careful to prevent personal information from entering the public domain. Such information could compromise an individual’s professional position or bring the school into disrepute. On no account should staff members communicate with pupils or ex-pupils through these methods.

It is highly advised that staff members set their social networking accounts to “private” to reduce risk. To set your Facebook profile to “private”, select the “Home” arrow at the top right of the screen. If you want friends to see your profile, select “Friends”. Now your profile is private to everyone except your current friends. Please contact the ICT Subject Leader for any support regarding privacy settings.

**School Website**

The school website is a platform for the school to share information with parents in an efficient way. Nominated members of staff are responsible for updating the website on a regular basis. Any new content that is to be uploaded to the school’s website must be proofread to identify any grammatical errors and then checked by team leaders. It is the uploader’s responsibly to ensure that the school has parental consent for any children’s photographs that are used on the school website. A comprehensive list of parental consent can be collected from the office.

**Access lanyards and door code**

Members of staff are issued with door codes and access lanyards to enter specific areas of the school. It is vital that these codes are not shared with the children. **Access lanyards should never be left unattended or given to children.**

**Children**

**Social Networking and E-communications**

The computing curriculum aims to teach children how to: use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact. In order to achieve this aim, teachers must ensure children are aware of the risks of social networking and e-communications.

Children will be prohibited from using any social network websites/apps or personal email addresses in school. Although children are restricted from using social networking in school, it is important that staff are aware children may use these services outside of school. Children should be encouraged to report to parents/teachers any attempts by people who they don’t know to contact them or if any bullying and threatening behaviour is directed towards them. Any issues that are reported must be passed on to the class teacher and Head Teacher immediately. Children will be taught to never give out their email address in a public setting (virtual or real), or to divulge personal details in public Internet spaces. This will be reinforced whenever the Internet is used through continued verbal reference and visual reminders.

*“There were 7,296 counselling sessions with young people who talked to ChildLine about online bullying and safety last year.” (NSPCC, 2016)*

**Printing and file storage**

All members of staff will be provided with a unique printing code. When printing, machines will request your code to authorise the job. Children will not be provided with the code, and must ask an adult to confirm their printing by entering their code. This code must be kept safe, and be used responsibly to reduce paper waste.

Children will have access to the *mydesktop* space to save their files. Inappropriate materials or text found on *mydesktop* should be reported and the child’s access to ICT may be temporarily suspended, and only reinstated following discussion with, and agreement by, the parents. The children will be taught how to use the space to create a portfolio of their work and links to copies of resources that they use to complete their schoolwork. Administrators reserve the right to access personal *mydesktop* space when requested by the Head Teacher.

**Additional Information**

**Parent involvement**

Parents will be kept informed of use of and developments in ICT through:

* School prospectus
* Acceptable use agreement
* School website and newsletter

The school will consider the specific religious views of some families on the use of technology.

Any concerns regarding the use and teaching of ICT should be addressed to the class teacher in the first instance and referred to the Head Teacher if necessary.

**Admin Network**

The school adheres to the LA policy regarding use of the administration machines.

**Community Use**

As an extended school, community users may need to access the school ICT network during parental afternoons, workshops, Sure Start, family learning and adult courses.

Community users cannot access any school shared areas or documents.

**Other**

Use of the network for personal monetary profit or gambling is strictly forbidden.

In accordance with the Data Protection Act 1984/98, users are not allowed to access other users’ personal files and folders, the exception to this being system administrators who can gain access through permission from the Head Teacher when just cause has been established.