



Bankfields Primary School

Policy for the Safe use of ICT

Head teacher – Mrs E Gatenby	
Review Date	September 2025
Chair of Governors – Mrs M Mockler	
Next Review Date	September 2026

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. As stated in the ‘Keeping Children Safe in Education’ (KCSIE) 2025 document, the breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The internet is to be used in a manner that is consistent with government guidance. Children, young people, and indeed adults, may encounter a range of risks online, these are identified within the ‘Keeping Children Safe in Education’ (KCSIE) 2025.

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. ICT equipment and resources within this school are provided to enhance pupils' learning and to guide staff in their delivery of 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.

Roles and Responsibilities – The School

As a school, we aim to ensure parents and pupils are fully aware of different ways in which the internet and ICT can be used safely and effectively. We will ensure that we always provide the opportunities for children to excel in ICT and ensure that our curriculum is relevant and challenging. Children's safety will always be at the forefront of our lessons and parents will be informed when necessary through newsletters and parents events.

Roles and Responsibilities – ICT Coordinator

The ICT coordinator will be responsible for overseeing planning in all year groups throughout the school and for raising standards in ICT. They will be responsible for informing staff of important and current information that is new and developing, and providing relevant staff with training when necessary. They will also oversee the assessment of ICT and monitor progress, software licensing, managing equipment, keeping regular contact with OneIT support and providing guidance for future purchasing of equipment.

Roles and Responsibilities – Teachers

Class teachers are responsible for recording pupils' progress following curriculum assessment, and for planning and teaching relevant computing lessons. Teachers are responsible for using ICT on a regular basis, ensuring they are using their interactive whiteboard to provide visual stimulus for learning and providing opportunities to use iPads. All teachers should report and respond to any e-safety or cyberbullying issues that they encounter.

Internet Safety

Filtering

Statutory guidance from the 2025 update of KCSIE dictates the following:

5. *Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.*

Filtering and monitoring expectations in schools and education settings have been updated in the document 'Meeting digital and technology standards in schools and colleges':

6. *The Department for Education's filtering and monitoring standards set out that schools and colleges should:*

- *identify and assign roles and responsibilities to manage filtering and monitoring systems.*
- *review filtering and monitoring provision at least annually.*
- *block harmful and inappropriate content without unreasonably impacting teaching and learning.*
- *have effective monitoring strategies in place that meet their safeguarding needs.*

Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

Additional guidance on "appropriate" filtering and monitoring can be found at: UK Safer Internet Centre: <https://saferinternet.org.uk/guide-and-resource/teachersand-school-staff/appropriate-filtering-and-monitoring>. The UK Safer Internet Centre produced a series of webinars for teachers on behalf of the Department. These webinars were designed to inform and support schools with their filtering and monitoring responsibilities and can be accessed at Filtering and monitoring webinars available – UK Safer Internet Centre.

South West Grid for Learning (swgfl.org.uk) has created a tool to check whether a school or college's filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content, Your Internet Connection Blocks Child Abuse & Terrorist Content).

7. *Online safety and the school or college's approach to it should be reflected in the child protection policy which, amongst other things, should include appropriate filtering and monitoring on school devices and school networks. Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and smart technology, which will also reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.*

In line with DfE guidance, the school has appropriate filtering and monitoring systems in place. The school's broadband connection is provided by OneIT. The filters in place are

extensive and include lists of illegal sites/inappropriate sites that cannot be accessed. It also allows open access and sharing of resources between educational establishments. Use of the internet through OneIT's services (using Securly Filtering and Monitoring) is monitored and traceable by the network administrators, including alerts provided to the DSL/DDSLs (Mrs Gatenby, Mrs Lee and Mrs Ward) in the event of access to websites that may contain inappropriate content. In addition to this, there is the consideration that children will inevitably access the internet outside of school. It is therefore vital that we give our children the tools and knowledge to empower them to be safe on the internet and equally as important - to know what to do when they come across any of the dangers. This is addressed further below.

From time-to-time, websites can be blocked even though there are no obvious threats or dangers. Once these have been checked thoroughly by a member of staff, they can contact the OneIT Helpdesk to notify them that a website is suitable for educational purposes. This can be done at: <https://portal.oneitss.org.uk/#/>. Staff have account log in details for this purpose.

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. Teachers 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.

Staff need to be vigilant as to the different sites children are accessing, making sure that children are not left unattended when using the internet. 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. The teaching of internet use and other aspects of e-safety will be covered within the computing curriculum. Staff are encouraged to engage in regular dialogue with the pupils that explores the benefits and potential dangers of using the internet. 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. If users, especially children, see an inappropriate website or image, they should minimise the page immediately and report the site to their class teacher, who will report this to the ICT coordinator. The ICT coordinator will then attempt to get this site blocked.

Accessing and interacting with the Internet is part 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 regularly 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/webpace and the impact of a digital footprint
- Copyright
- What to do when you come across something that is inappropriate
- How to proceed if bullying/inappropriate communications are made

Remote Learning

For home learning, children will be provided with opportunities to do independent tasks using Seesaw. Children will be expected to return work assignments through an online platform to demonstrate they have met their learning target and completed their task to the same high standard they would in school. While we offer opportunities for children of all abilities to develop their skills and knowledge, we also ensure that the children are increasingly challenged. Tasks will be sent directly to Seesaw with any additional information included with the given task, tasks may include, images, videos, audio etc.

Parents are able to monitor and support children academically and help them to use online resources responsibly and safely on through the use of their own personal login. Children will receive feedback on their engagement and learning, and that will be the same for children in the remote learning pathway as those in the in-person learning pathway.

The teacher will:

- Set weekly home learning activities which will be an extension of their school learning and compliment their current creative curriculum topic
- Give feedback and praise
- Set high expectations of pupils in completing remote learning tasks
- Record and monitor tasks completed
- Provide additional resources should this be deemed necessary

Parents/carers should:

- Provide a suitable learning place
- Ensure that home learning tasks are completed on time and to a suitable standard
- Encourage pupils and praise them when they have completed home learning task
- Contact the child's class teacher if they have any questions

Children should:

- Complete their learning task to the best of their ability.
- Take care with the presentation of their work
- Complete it as well as they can
- Ask for help from their parents/carers and older brothers/sisters
- Speak to the class teacher if there was anything they didn't understand

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.

Username (example): RBPMKelly@bankfields.steelriver.org.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.

All members of staff must check their emails frequently to ensure that they are up-to-date with events. Staff must also check the calendar linked to their emails frequently, and ensure that any key information/events are put onto the calendar email.

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 and all staff (teaching, support and admin) mobile phones should be on silent during school hours. They should not be accessible to children and are not allowed in classrooms. Private telephone calls should only be made or taken during break and lunch times unless an emergency and must 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.

When telephone contact has been made with parents, it has been strongly encouraged that this be done in school and using the school's telephone. Staff who have chosen to telephone parents from home, it has been made clear that personal details be withheld using the phone's settings or by dialling with the prefix '141'.

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 Instagram 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. Staff need to ensure that they report any incident with the Head teacher.

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. Staff need to carefully consider whom they accept as friends on social media.

School Website and Facebook

The school website and Facebook account 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 and Facebook account on a regular basis. Any new content that is to be uploaded to the school’s website and Facebook must be proofread to identify any grammatical errors and then checked by team leaders. It is the uploader’s responsibility 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. If a lanyard is lost, staff must immediately alert the reception desk, and they will disarm the lanyard.**

USB Drives and External Hard Drives

Members of staff are prohibited from using USB Drives and External Hard Drives to store and transfer data within school. USB storage devices are easily lost or stolen, putting any data they contain at great risk of being accidentally or deliberately exposed.

The loss of confidential or sensitive personal data on a USB storage device results in a breach of the school’s safeguarding policy.

GDPR

The school takes its role with the General Data Protection Regulation (GDPR) seriously and aims at all times to ensure personal data is secure and safe.

Staff will not be permitted to discard or copy sensitive or personal digital data from School network unless the data storage device is encrypted and is transported securely for storage in a secure location.

Paper based protected and restricted data must be held in a lockable storage. Staff must make sure they have a relevant and valid purpose to have any data in print and if data has been printed off it needs to be securely disposed of once it is no longer required into the red bins. Staff should ensure they do not leave information unattended.

Any user that sends email attachments containing private, personal or sensitive data must encrypt this via content encryption and it is the user's responsibility to ensure that this happens. The user will be provided with the necessary information and passwords to enable them to encrypt files.

The Data Controller (Director of Operations) in the School is responsible for ensuring that personal data stored on School systems regarding staff, pupils and parents is appropriately restricted and only accessible to designated individuals. Staff are strictly prohibited from storing pupil or parent data on their own personal devices. Staff are therefore expected to act responsibly if using their personal mobile device for School business.

Staff must report any breaches of General Data Protection Regulation (GDPR) immediately. They must login to GDPRiS portal and log the incident. All staff have a login and password.

User (example): RBPMKelly@bankfields.steelriver.org.uk

Password: *****

The head teacher and GDPRiS Portal Manager will take relevant action to any issues and incidents raised.

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
- Bankfields Facebook Page

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.

Information and Support – ‘Keeping Children Safe in Education’ (KCSIE) 2024

There is a wealth of information available to support schools, colleges and parents to keep children safe online. The following list is a starting point for some support:

Organisation/Resource	What it does/provides
https://www.thinkuknow.co.uk	NCA CEOPs advice on online safety
https://www.disrespectnobody.co.uk/relationship-abuse/what-is-relationship-abuse/	Home Office advice on healthy relationships, including sexting and pornography
https://www.saferinternet.org.uk/	Contains a specialist helpline for UK schools and colleges
https://swgfl.org.uk	Includes a template for setting out online safety policies
https://www.internetmatters.org/?gclid=EAlaQobChMIktuA5LWK2wIVRYXVCh2afg2aEAAAYASAAEgIJ5vD_BwE	Help for parents on how to keep their children safe online

https://parentzone.org.uk/	Help for parents on how to keep their children safe online
https://www.childnet.com/resources/cyberbullying-guidance-for-schools	Guidance for schools on cyberbullying
https://www.pshe-association.org.uk	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
https://educateagainsthate.com	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
https://www.gov.uk/government/organisations/uk-council-for-internet-safety	The UK Council for Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/e-safety-schools/	NSPCC advice for schools and colleges
https://www.net-aware.org.uk	NSPCC advice for parents
https://www.common sense media.org	Independent reviews, age ratings, & other information about all types of media for children and their parents
https://www.gov.uk/government/publications/searching-screening-and-confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
https://www.lgfl.net/online-safety/default.aspx	Advice and resources from the London Grid for Learning