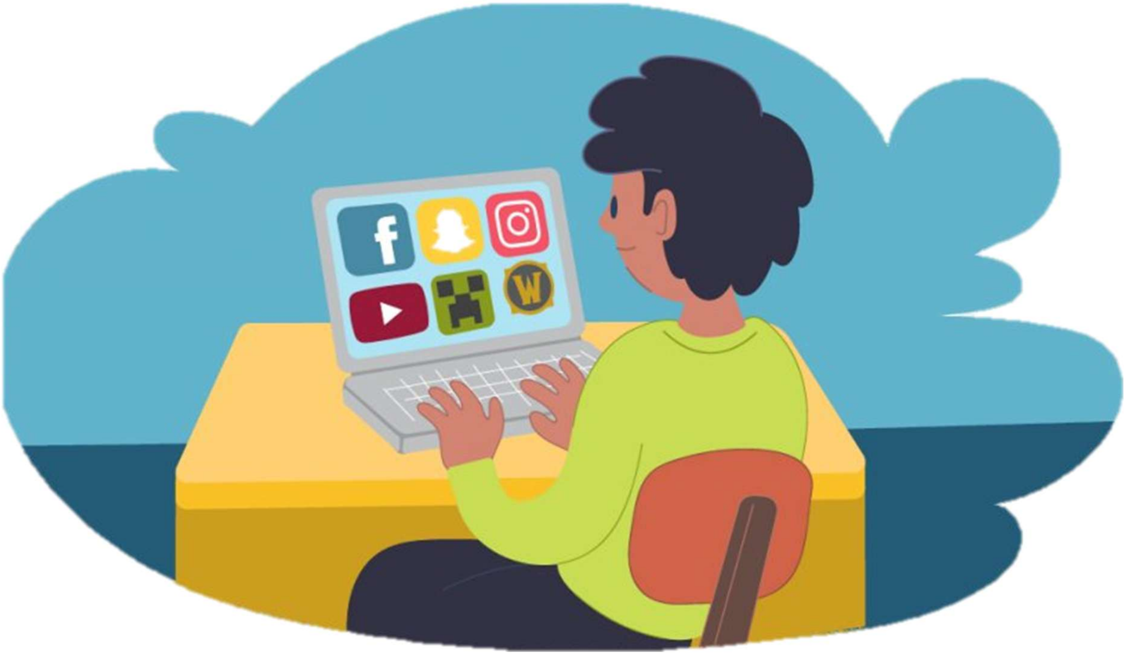
Bankfields Primary School

Online Safety Policy



September 2025

Review date: September 2026

Online Safety

The school has a Designated Computing and Online Safety Leader (M Smith), who is responsible for reviewing and updating this policy. They work in collaboration with the Safeguarding Team and members of the SLT in order to ensure this policy meets the ever-changing issues relating to the internet and its safe use.
The Online Safety Policy has been written by the school, incorporating points from the Department for Education's (DfE) statutory guidance 'Keeping Children Safe in Education', its non-statutory guidance 'Teaching Online Safety in Schools' and a number of other carefully selected sources. Key documents in school that inform this document and have, in turn, been informed by this document include the Steel River Academy Trust Safeguarding Policy and the Bankfields Child Protection Policy. This policy has been agreed by the leadership team and approved by the Governing Body. It will be reviewed regularly. Changes will be made immediately if technological or other developments require it.

Role of Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/MAT/relevant body
- liaises with school technical staff
- receives reports of online safety incidents on CPOMS
- reports regularly to Senior Leadership Team

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Our approach to online safety is based on addressing the following categories 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. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group

Online Safety Risks

The Department for Education published an updated version of 'Keeping children safe in education' in 2025. It states the following:

1. *All staff should be aware of the indicators of abuse, neglect and exploitation (see below), understanding that children can be at risk of harm inside and outside of the school/college, inside and outside of home, and online. Exercising professional curiosity and knowing what to look for is vital for the early identification of abuse and neglect so that staff are able to identify cases of children who may be in need of help or protection.*

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content.

2. *It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff* *in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.*

3. *The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:*

3.1 *<u>content:</u> being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.*
3.2 *<u>contact:</u> 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.*
3.3 *<u>conduct</u>: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and*
3.4 *<u>commerce:</u> risks such as online gambling, inappropriate advertising, phishing and or financial scams.*

The KCSIE document for 2025 includes aligning the definition of safeguarding used with that in Working Together to Safeguard Children (2023). This makes explicit reference to online activity:
3.5 *No single practitioner can have a full picture of a child's needs and circumstances. If children and families are to receive the right help at the right time, everyone who comes into contact with them has a role to play in identifying concerns, sharing information and taking prompt action. Safeguarding and promoting the welfare of children is defined for the purposes of this guidance as:*
• Providing help and support to meet the needs of children as soon as problems emerge
*• protecting children from maltreatment, **whether that is within or outside the home, including online***
• preventing the impairment of children's mental and physical health or development
• ensuring that children grow up in circumstances consistent with the provision of safe and effective care
• taking action to enable all children to have the best outcomes.

Furthermore, the importance of staff understanding the role that children can play in abusing other children is highlighted in the document:

4 *All staff should be aware that children can abuse other children (often referred to as child-on-child abuse), and that it can happen both inside and outside of school or college and online. All staff should be clear as to the school or college's policy and*

procedures with regard to child-on-child abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it.
More detail on this matter is included in the school's Safeguarding Policy.

The following sections of this policy address the above risks and the systems in place to reduce the risk both within school and for our children in their home lives.

Filters and Monitoring

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 assessed 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 (Securly Filtering and Monitoring) 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 is monitored and traceable by the network administrators, including alerts provided to the DSL/DDSL (Mrs Gatenby, Mrs Lee, 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.

Searches using the school's network are monitored. The school uses Securly to notify the headteacher of any inappropriate searches or searches which then result in accessing a site with potentially inappropriate content. The headteacher will then follow up any of these breaches and a log is held by the DSL.

In 2024, the DfE also provided an update entitled 'Cyber security standards for schools and colleges'. This is relevant here as it references 'safeguarding issues due to sensitive personal data being compromised' and states:
The cyber security standards have been updated to address tasks that should be completed by both the senior leadership team (SLT) and IT support. Cyber security is not something that IT teams can carry out alone, it is a shared responsibility between multiple roles and teams.

In addition, the 2025 update of KCSIE includes reference to the Department for Education's guidance on generative AI, 'Generative AI: product safety expectations' (2025). This guidance outlines product safety expectations and supports schools in understanding their filtering and monitoring responsibilities when using AI technologies.

Cyberbullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHRE, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

Online Safety Education & Training

Whilst regulation and technical solutions are very important, their use must be balanced by educating users of potential Online Safety risks as well as how to develop safe and responsible behaviours to minimise them, wherever and whenever they go online.

Online Safety education will be provided in the following ways:

Online Safety Training for Staff and Governors

At Bankfields Primary School we ensure that all teaching and non-teaching staff can recognise and are aware of Online Safety issues. All staff take responsibility for promoting online safety. They are directed to relevant websites to help support their understanding of these issues. All members of staff are also aware of the documents and policies which have to be updated throughout each year and where their actions need to be monitored and logged (see managing online safety). During each September, each member of staff reviews the policies for both online safety and acceptable use and they also review the statements which underpin their Acceptable Use Agreement and Staff Behaviour Policy.

The 2025 update to KCSIE states:
8. *Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. It is not appropriate for the proprietor to be the designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description.*
*Governing bodies and proprietors should ensure that all governors and trustees receive appropriate safeguarding and child protection (**including online**) training at induction. This training should equip them with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures in place in schools and colleges are effective and support the delivery of a robust whole school approach to safeguarding. Their training should be updated regularly.*

Online Safety Training for Parents

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

For these reasons, the school provides opportunities for parents/carers to receive online safety education and information (e.g. via the school website, Facebook and Parent Mail) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good online safety behaviour. Parents also receive online safety training through our Family Learning Events using resources produced by 'Online Safety' (Alan Mackenzie).

E-Safety

An Online Safety (e-Safety) curriculum will be established in computing and PSRHE sessions, and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils, and teach children how to minimise the risk when working on the internet. All children will be regularly informed on how to use the internet safely, covering both safe school and home use.

Children will have the opportunities discuss various e-safety procedures, they will be reminded of online safety messages; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials. They will also be taught how to use a range of age-appropriate online tools in a safe and effective way. Staff will ensure that they model safe and responsible behaviour in their own use of technology during lessons.

Children will be made aware of where to seek advice or help if they experience problems when using the Internet and related technologies. If a teacher suspects an E-safety issues within the school they should ensure that this is reported immediately to the ICT coordinator and head teacher.

Social Networking

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.

Dealing with exposure to inappropriate materials: content, contact and conduct

Guidance to staff

If you suspect or are told about a content, contact or conduct, including cyber-bullying, incident, follow the protocol outlined below:

Mobile Phones

- Ask the pupil to show you the mobile phone.
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names.
- Make a transcript of a spoken message, again record date, times and names
- Tell the pupil to save the message/image (if appropriate).
- Go with the pupil and see the Head teacher, or in her absence, a member of the Senior Leadership Team.

Computers

- Ask the pupil to get up on-screen the material in question (if this is not possible the child could tell you how to find it on the screen and the website they were working within).
- Ask the pupil to save the material (if appropriate).
- Print off the offending material as a record (cyberbullying).
- Make sure you have got all pages in the right order and that there are no omissions.
- Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented.

Guidance for Pupils

- If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, a teacher or your headteacher.
- Do not answer abusive messages but log and report them.
- Do not delete anything until it has been shown to your teacher, parents/guardian or the headteacher (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying).
- Do not share personal IT details.
- Never reply to abusive e-mails, messages or texts.
- Never reply to someone you do not know.

Guidance for Parents

It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyberbullying:

- Parents can help by making sure their child understands the school's policy and, above all, how seriously Bankfields Primary School takes incidents of cyber-bullying.
- Parents should also explain to their sons or daughters legal issues relating to cyberbullying.
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents should contact the Head teacher as soon as possible. A meeting can then be arranged, which may involve other relevant members of staff.

If any teacher, pupil or parent suspects that any of our children are at heightened risk of exposure to inappropriate use of the internet, they should inform the Designated Safeguarding Leads as a priority.

Online Safety at home

In line with the school's approach to all aspects of safeguarding, parental engagement is considered essential in ensuring children are safe online. The school believes that parents are their children's first and best teachers and that they need to be equipped with the knowledge and skills to support their children at home. Updates on an aspect of online safety relevant to primary school children are sent home via Parent Mail and uploaded onto Facebook. In addition, more detailed half-termly resources are provided, for example our 'Online Safety Leaflet for Parents' and Vodafone's 'Digital Parenting' magazine.

Several sites offer helpful advice to parents, particularly with respect to how they can best monitor their child's use of the computer at home. Some examples of important and useful information that the school has shared with parents can be found on the following sites:

- www.thinkuknow.co.uk/
- www.saferinternet.org.uk
- www.net-aware.org.uk
- www.parentzone.org.uk
- http://vodafonedigitalparenting.co.uk/

Acknowledgements:

Keeping children safe in education: Statutory guidance for schools and colleges. (2025) Department for Education. https://assets.publishing.service.gov.uk/media/686b94eefe1a249e937cbd2d/Keeping_children_safe_in_education_2025.pdf [Accessed 25 July 2025]