**Bankfields Primary School**

**Online Safety Policy**



**September 2024**

**Review date: September 2025**

**Online Safety**

The Designated Safeguarding Lead takes overall responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place.

The school has a Designated Computing Subject Leader (M Smith), who reviews and updates this policy alongside the Designated Safeguarding Lead. The Computing Subject Leader works in collaboration with the Designated Safeguarding Lead, 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. The 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 / DSL**

* 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**

In The Department for Education’s ‘Keeping Children Safe in Education’, it states the following:

* *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.*
* *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.*
* *The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk (content, contact, conduct and commerce):*
	+ *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: 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*
	+ *commerce: risks such as online gambling, inappropriate advertising, phishing andor financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).*
* *Schools and colleges should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.*
* *Resources that could support schools and colleges includes:*
* *DfE advice for schools: teaching online safety in schools;*
* *UK Council for Internet Safety (UKCIS)Education for a connected world; 32 guidance:*
* *UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people;*
* *The UKCIS external visitors guidance will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors;*
* *National Crime Agency's CEOP education programme: Thinkuknow;*
* *NSPCC Learning - Undertaking remote teaching safely during school closures*
* *PSHE - PSHE Association coronavirus hub*

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 DfE (KCSiE) states the following:

* *Governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the above risks from the school’s or college’s IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectivemess.* *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 age range of their children, the number of children, how often they access the IT system and the proportionality of costs versus risks.*
* *The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. UK Safer Internet Centre: appropriate filtering and monitoring. 33 The UK Safer Internet Centre has published guidance as to what “appropriate” filtering and monitoring might look like:*

In line with DfE guidance, the school has appropriate filtering and monitoring systems in place. The school’s 200mb broadband connection is provided by One IT, who also provide our filtering and monitoring services. The filters and monitoring are extensive (Securly Filtering and Monitoring) and include lists of illegal sites/inappropriate sites that cannot be accessed. Senior Leaders are alerted by email if a prohibited site or search has been detected so that it can be followed up. 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 internet in school is monitored and traceable by our filtering and monitoring systems. 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.

**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. The DSL and Computing Lead complete training around Online Safety, which is then disseminated to all staff and governors.

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). 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.

**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 an up-to-date ‘Online Safety Guide for Parents’ that has been produced by the school. We also arrange for our parents to receive copies of the ‘Digital Parenting’ magazine (published by Vodafone and ordered from Parentzone) which covers current and relevant issues linked to the use of internet use when these are published.

**E-Safety**

An Online Safety (e-Safety) curriculum will be established in computing and PSHRE 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. (2024) Department for Education.

<https://assets.publishing.service.gov.uk/media/66d7301b9084b18b95709f75/Keeping_children_safe_in_education_2024.pdf>