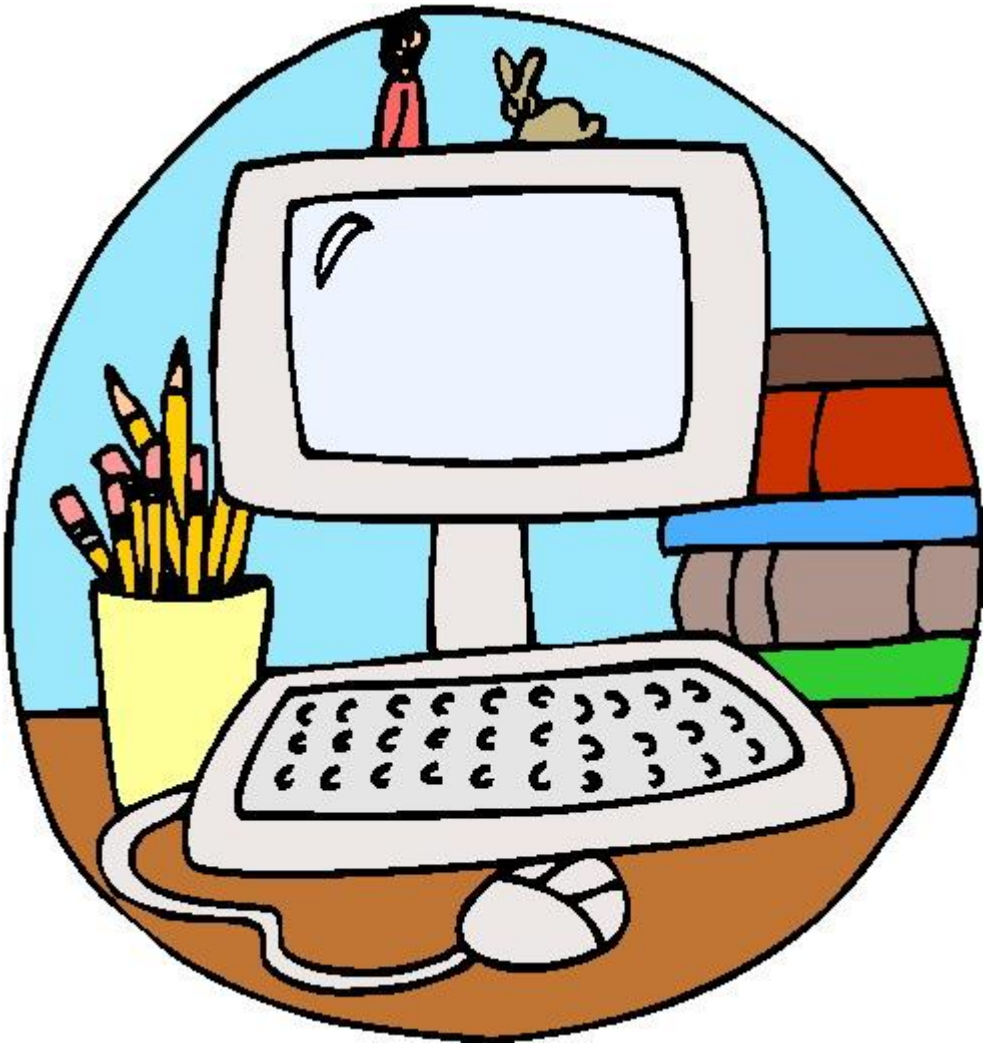
Bankfields Primary School

Computing and Online Safety Policy



2021 - 2022

Computing at Bankfields Primary School

This policy sets out our school's vision, aims, principles and strategies for the delivery of Computing and the use of technology to support the curriculum at Bankfields Primary School and should be read in conjunction with the 'Policy for the Safe use of ICT'. This policy was written in 2020 and will be reviewed every two years. This policy should be read in alliance with the following documents:

- Computing key concepts document
- Computing whole school key knowledge progression document
- Computing individual long term plans

Curriculum Intent

At Bankfields, our intent for computing provision is to prepare our pupils for the digital world. We want to develop the children's understanding of the digital world that they live in, and help them to develop the skills and knowledge they need to pursue their love of computing in both education and the world of work. Our computing curriculum is designed to help promote our children to become positive citizens, who communicate respectfully online in both the society we live in and in school by completing termly online safety lessons that explores a wide range of topics such as, digital footprints, terms and conditions, online bullying and fake news. As a school, we have numerous visitors from the computing work force that develop new skills with the children and help establish an interest in a computing role for our children in the future. During lessons, children are taught many computing skills that are essential in allowing children to be confident, creative and independent learners such as understanding the use of the internet, how we store digital content, input and output, the use of computer networks and how we can present information using different software. Children are given the opportunity to design and create their own algorithms, debug algorithms, evaluate algorithms, whilst continuing to broaden their use of computational language. This may be seen through Bee-Bot activities, physical algorithms, sorting cards and Espresso coding activities. It is our intent at Bankfields, for our children to be confident with the computing skills they have learnt, so that they can be used outside of school and further in their education and careers.

Computing at Bankfields Primary School

At Bankfields Primary school, our aim is to produce learners who are confident, effective users of technology and who also are equipped with the confidence and capability to use ICT and computing throughout their later life. We recognise and respond to new developments in technology and use ICT and computing as a tool to enhance learning throughout the curriculum. We are committed to a high quality and sustainable programme of Computing teaching across the school, which is accessible to all children at their own level. At Bankfields, we aim to develop the understanding of how to use ICT and computing safely and responsibly. Our

teachers are encouraged to progressively develop pupils' Computing skills and capability through relevant, challenging and enjoyable curriculum for all pupils.

Our Computing curriculum, meets the requirements of the National Curriculum programmes of study for computing and is integrated into the curriculum and used as a truly beneficial tool for learning.

The national curriculum for computing aims to ensure that all pupils:

- Can understand and apply the fundamental principles of computer science, including logic, algorithms, data representation, and communication
- Can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems
- Can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems.
- Are responsible, competent, confident and creative users of information and communication technology.

Inclusive teaching of Computing

At Bankfields Primary School, we teach computing to all children, whatever their ability, age, gender or race. Computing forms part of our school curriculum policy to provide a broad and balanced education for all children. Each pupil's access to technology varies greatly dependent on the nature of the activity they are involved in. All children have equality of access to appropriate technology in order to develop their personal Computing capability. Teachers are regularly advised on examples of technology which can be provided to support individual children with particular physical, linguistic and educational needs.

Computing and Special Educational Needs Pupils

At Bankfields Primary School, we believe that all children have the right to access ICT and computing. We provide learning opportunities that are matched to the specific needs of children with learning difficulties. Consequently, in some instances, the use of ICT has a considerable impact on the quality of work that children produce; it increases their confidence and motivation and allows access to parts of the curriculum to which the children would otherwise not have had. Through the teaching of ICT and computing we provide learning opportunities that enable all pupils to make progress. We do this by setting suitable learning challenges and responding to each child's different needs. Where appropriate ICT and computing can be used to support SEN children on a one to one basis where children receive additional support. Additionally as part of our dyslexia friendly approach to teaching and learning we will use adapted resources wherever possible such as visual timetables, different coloured backgrounds and screen printouts.

Objectives

Computing in Foundation Stage

In the EYFS, opportunities for the use of technology are an integral part of each area of learning and the school ensures that children have access to this provision. It is important in the foundation stage to give children a broad, play-based experience of computing in a range of contexts, including outdoor play. ICT is not just about computers. Early years learning environments should feature ICT scenarios based on experience in the real world, such as in role play. Recording devices can support children to develop their communication skills. This is particular useful with children who have English as an additional language.

Computing in Key Stage 1

Key Stage 1 children are using a scheme of work which has been designed by the Computing leader and teachers from across school. The scheme of work ensures that by the end of Key Stage 1 pupils should be taught to:

- Understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions.
- Write and test simple programs.
- Use logical reasoning to predict and computing the behaviour of simple programs.
- Organise, store, manipulate and retrieve data in a range of digital formats.
- Communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school.

Computing in Key Stage 2

Key Stage 2 children are using a scheme of work which has been designed by the Computing leader and teachers from across school. In order to create this scheme of work, the Computing lead consulted with a KS3 ICT specialist to design a curriculum which will give pupils the passion and basic ICT learning skills needed for KS3. The curriculum is linear and set out in the Computing key concept document, Computing whole-school key knowledge progression document and Computing individual long-term plans. The scheme of work ensures that by the end of Key Stage 2 pupils should be taught to:

- Design and write programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts.
- Use sequence, selection, and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs.
- Use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs.
- Understand computer networks including the internet; how they can provide multiple services, such as the world-wide web; and the opportunities they offer for communication and collaboration.

- Describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely.
- Select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

Assessment and Monitoring of Computing

Teachers regularly assess capability through observations and looking at completed work. Teachers assess mostly at the end of each unit of work. Judgments are formed through assessing the children's work in Computing by making informal judgements as we observe the children during lessons. Use of independent open ended tasks, provide opportunities for pupils to demonstrate capability in relation to the term's work. These are often evidenced in the class teachers' floor book half-termly or within the children's curriculum books.

Throughout the academic year, class teachers can use the supporting documentation to establish whether a child has achieved the curriculum intent.

The subject leader is responsible for monitoring the standard of the children's work and the quality of teaching in line with requirements from subject leader meetings, work analysis and lesson observations. The subject leader is also responsible for supporting colleagues in the teaching of computing, for being informed about current developments in the subject, and for providing a strategic lead and direction for the subject in the school. It is the responsibility of the subject leader to monitor the progress of Computing across the school with reference to specific action points outlined in the Computing action plan.

Resources

Hardware

At Bankfields, a range of resources are available, which successfully supports delivering the Computing curriculum and enables all learners to reach their full potential. We acknowledge the need to continually maintain, update and develop its resources and to make progress towards a consistent, compatible system by investing in resources that will effectively deliver the strands of the national curriculum and support the use of computing across the school. All classes have one computer or laptop in their room which is connected to the school network and gives access to school resources, software and the Internet. Each class has an Interactive Whiteboard which has replaced the traditional whiteboard. The children have access to a range of Computing equipment across school including desktop computers, laptops and iPads. All hardware appliances are audited each year and updated as hardware is changed or added. At Bankfields we have a commitment to renew equipment regularly to reflect current and

developing technologies. Resources are suitably maintained and replenished when needed, which is overseen by the Computing Leader and ONEIT. Teachers are required to inform the computing coordinator of any faults as soon as they are noticed; these then, can be passed on to the relevant technical support. Resources, if not classroom based, are located in either computing suite.

Mobile Phones

The use of mobile phones and other digital devices by pupils in school is not permitted. Phones brought to school by pupils are done so at the owner's risk and are the responsibility of the pupil. Pupils who do bring phones into school, will be asked to take them to the school reception, where they will be securely stored until the end of the school day when they can be collected. The use of mobile phones by staff is only permitted when pupils are not present or in the staff room.

Interactive Whiteboards

Each class within school has an Interactive Whiteboard and teachers are monitored to ensure they are being used to their full potential. Where appropriate, lessons make use of digital resources and are interactive as to ensure that the children are fully stimulated and enthused.

Software

A wide-range of software is available on the network to suit the varied curriculum that we cover. There is a suitable selection of software available to facilitate the teaching of computing and create cross-curricular links.

Roles (see 'Policy for the Safe use of ICT' also)

Subject Leader of Computing

The subject leader is responsible for providing professional leadership and management of computing within the school. They will monitor standards to ensure high quality teaching, effective use of resources and improved standards of learning and achievement. This will include observation of lessons and monitoring of the pupils' work. To offer help and support to all members of staff (including teaching assistants) in their teaching, planning and assessment of computing. They will collect, analyse and distribute, where applicable, information relating to the subject to the relevant people. It is their responsibility to lead staff training on new initiatives; attend appropriate in-service training and keep staff up to date with relevant information and development; and keep parents informed and give them guidance on any relevant online safety issues.

Class Teachers

It is the responsibility of each class teacher to ensure that their class is taught all elements of the computing curriculum as set out in the National Curriculum programme of study; Key knowledge; and Key concepts grids. At Bankfields Primary School we set high expectations for our pupils and provide opportunities for all pupils to achieve, including girls and boys, pupils

with educational special needs, pupils with disabilities pupils from all social and cultural backgrounds making sure they are setting suitable targets for learning. The class teacher's role is a vital role in the development of computing throughout the school and will ensure continued progression in learning and understanding, ensuring they keep up to date assessment records, including through the use of 'floor books'.

Parental involvement

Parents are encouraged to support the implementation of ICT and computing where possible by encouraging use of computing skills at home during home-learning tasks and through the school website. They will be made aware of e-safety and encouraged to promote this at home.

Training

All staff, including managerial and administrative staff, receives support from the subject leader or technicians. At Bankfields Primary, the Computing subject leader will assess and address staff training needs as part of the annual development plan process or in response to individual needs and requests throughout the year. Individual teachers should attempt to continually develop their own skills and knowledge, identify their own needs and notify the coordinator. Teachers will be encouraged to use ICT to produce plans, reports, communications and teaching resources.

Online Safety

The school has a Designated Computing and Online Safety Leader (M Kelly), 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. 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

- 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 2021. It states the following:

- *Technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic 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)*
- *Schools and colleges should ensure online safety is a running and interrelated theme whilst devising and implementing 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 dictates 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. 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 vs 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:*

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.

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.

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 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. (2021) Department for Education. https://www.gov.uk/government/publications/keeping-children-safe-in-education--2