Online Policy Summary

Introduction
At Bankwood Primary School we understand the responsibility we have to educate our pupils on online safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

We have a whole school approach to the safe use of ICT and creating this safe learning environment includes three main elements:

- an effective range of technological tools
- policies and procedures, with clear roles and responsibilities
- a comprehensive on-line programme for pupils, staff and parents.

This policy has been contributed to by the whole school and ratified by the governors.

This policy is to be read in conjunction with all other policies particularly: Behaviour Policy, Safeguarding Policy and Child Protection Policy and Code of Conduct policy

Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in Bankwood Primary School.
The Headteacher has overall responsibility. The Inclusion team are named staff for children to report any concerns; although, any member of the Bankwood staff have the responsibility to be aware children could report to them too.
It is the role of all staff members to keep abreast of current issues and guidance through organisations such as Sheffield LA, CEOP (Child Exploitation and Online Protection), and Child Net. The Head teacher ensures Senior Management and Governors are updated as necessary. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

All staff should be familiar with the school's policy including:
• safe use of e-mail (using bcc to keep addresses confidential)
• safe use of the Internet (ensuring they are always logged on as themselves and children under their own profile so that the filtering system is tailored to those individuals)
• safe use of the school network, equipment and data (when using VPN at home- ensuring logging off at the end of each session and using equipment provided only by the school to access VPN)
• safe use of digital images and digital technologies, such as mobile phones and digital cameras (see separate sexting policy) – parent consent is always agreed for use of digital imagery in school and on online platforms.

• publication of pupil information/photographs on the school website – parent consent is always agreed and given only to the website admin team when this has been given
• procedures in the event of misuse of technology by any member of the school community (see appendices)
• their role in providing e-safety education for pupils- This is one of the 4 units of work that MUST be taught using the lessons provided by the computing lead which has been agreed by SLT

Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for online guidance to be given to the pupils on a regular and meaningful basis. It has been planned into the Bankwood Computing Scheme of work as a separate strand. We continually look for new ways to promote online safety.

• We provide opportunities within a range of curriculum areas to teach about online safety.

• Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the curriculum.

• Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.

• Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the curriculum.

Managing access to the Internet

- Students will have supervised access to Internet resources through the school's fixed and mobile internet technology. Pupils have their own log on details and year 5 and 6 should be using this as their use of the internet will be more independent.
- Staff will preview any recommended sites before use and send any you tube clips they are unsure of to be checked by their KS lead first.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents re-check these sites and supervise any further research.
- Our internet access is controlled through Bluebox and if filtering needs lifting the site will have been checked by the teacher, phase leader and then the site taken to SLT and added to the list.
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately by the teacher or teaching assistant to a member of the safeguarding team.

It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

Any changes to filtering must be authorised by a member of the senior leadership team and Headteacher

Security and Data Protection

The school and all staff members comply with the Data Protection Act 1998. Personal data will be recorded, processed, transferred and made available according to the act. Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have secure passwords which are not shared with anyone. All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety Policy.

Online Safety Complaints/Incidents

As a school we take all precautions to ensure online safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this. Complaints should be made to the Headteacher. Incidents should be logged for managing an online safety incident is to be followed. It is important that the school work in partnership with pupils and parents to educate them about Cyber bullying and children, staff and families need to know what to do if they or anyone they know are a victim of Cyber bullying. All bullying incidents should be recorded and investigated through the Inclusion team. If an incident follows the below criteria
such as:

- using another person's user name and password
- using a mobile phone to take video during a lesson
- using the technology to upset or bully (in extreme cases this could be illegal- (see separate sexting policy)

The Headteacher and Safeguarding lead should be contacted immediately.

Remote teaching

As a school there may be rare circumstances when teachers will be asked to remote teach. Current guidance (NEU 2019) states,

- Teachers should not live-stream lessons from their homes, nor engage in any video-calling unless in exceptional circumstances, with the parent. Online lessons are not desirable for primary children as the teacher-pupil interaction is not easily replicated.

Current guidance (NEU- NASHT-edge) states,

- Schools must provide agreed platforms for staff to use and share information and resources, for example, Google Drive if the school is familiar with this.
  Agreed platform gmail y_@bankwood.sheffield.sch.uk

- Any contact between pupils and teachers should only be through a platform provided by the school and not through personalised accounts open to public viewing, comments or sharing. The NEU advises staff not to use or exchange personal email addresses or phone numbers with pupils.

- Any equipment provided by the school is for work purposes only and there must be shared agreements in place for pupils and parents on what behaviour and contact is appropriate, with clear sanctions for misuse.

Further information regarding our provision for remote learning can be found on the curriculum section of the website.