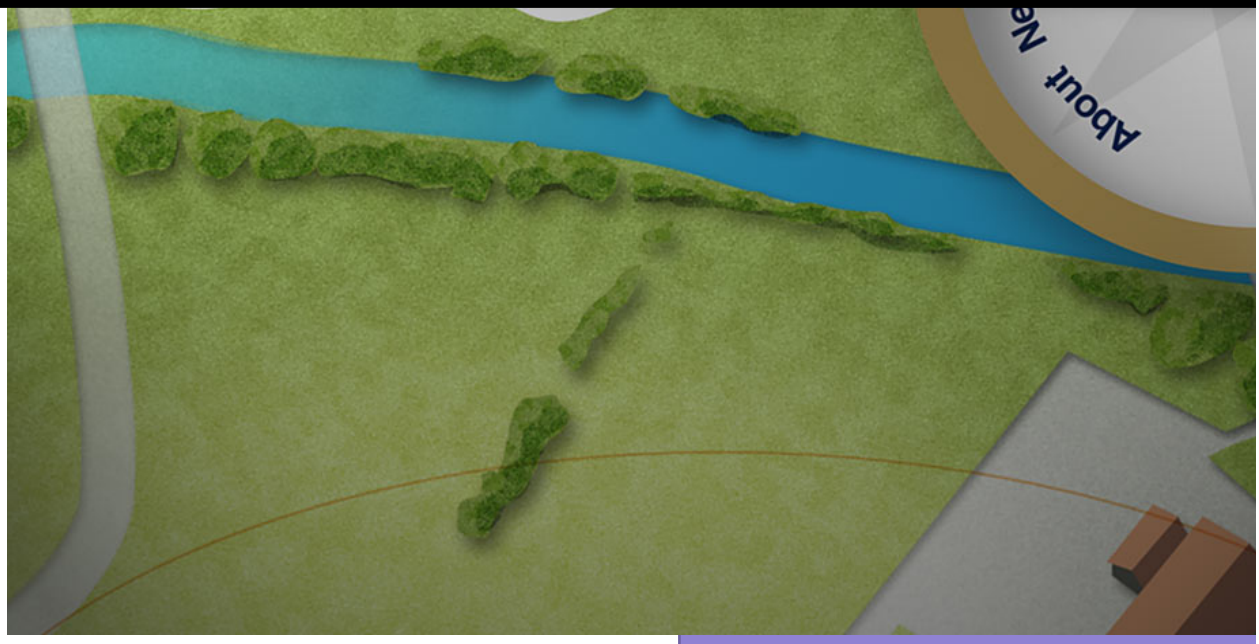
Northbrook Primary School On-line Safety Policy



Adopted by Governors/HT
Last Review Date : Febraury 2019
Next review : February 2020
Person Responsible : HT/ICT lead

Navigating pathways to success

On-Line Safety Policy

At Northbrook Primary School we are committed to using Information and Communication Technology and all it offers in the most effective and appropriate way, for the benefit of our pupils, staff and community. For this reason, we have developed this E-Safety Policy, to provide safeguards and ensure that all members of our school community understand the benefits, risks and what is expected of them when they use ICT in the learning environment. Our school internet access provider operates a filtering system that restricts access to inappropriate materials, however we also want informed pupils who know the dangers of information technology and know how to keep themselves safe.

Why internet use is important:

We believe the internet is an essential resource in 21st century life to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment.

Using the internet and ICT in general is a part of the statutory curriculum and a necessary tool for staff and pupils, therefore, school recognises its duty to provide children with quality internet access as part of their learning experience.

Pupils are increasingly using the internet and a range of ICT devices outside of school and therefore need to learn how to evaluate information and to take care of their own safety and security.

Learning:

Pupils will be taught what internet use is responsible and what is not and given clear objectives for internet use.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age group.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Online safety will be taught to all children at the start of the academic year and at the start of each half-term in designated online safety lessons. Online safety will also be

discussed where appropriate in all lessons where the use of digital technologies is incorporated.

Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.

Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended Instant Messenger and email addresses, full names of friends/family, specific interests and clubs etc.

Lessons will be used to educate pupils about cyber bullying, including how to report cyber-bullying.

Staying safe:

Internet based teaching is carefully planned to ensure that pupils are focussed and using appropriate and relevant materials.

Pupils may only use approved digital methods of communication on the school system.

Pupils do not have unsupervised access to the internet.

Pupils are taught what internet use is acceptable and what is not and given clear objectives for internet use.

Pupils are taught how to find appropriate information on the internet

Pupils and staff will use equipment responsibly.

Internet rules will be made a part of displays around school where appropriate.

Sanctions for inappropriate use of the internet will be explained to the children and will be tied into the school's behaviour policy. In the case of children who refuse to comply with expectations regarding online safety they will have their access to digital technologies restricted and will be provided with non-digital alternatives to allow them to access the curriculum.

E-mail

Although children are not issued with personal email accounts in school, we acknowledge that many children will have personal email accounts and so educate children to be aware of the benefits and risks and how to be safe and responsible users

On the occasions where email is used pupils will be taught:

- strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- that E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

How will social networking, social media and personal publishing be managed?

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and others.

Pupils have no access to social networking sites.

Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.

Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible using platforms such as Purple Mash.

Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

All pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

Parents will be kept informed of social media sites that school deems unsuitable for their children via newsletters and the online safety section of the school website.

School will inform parents about potentially harmful social media sites and apps but respects all parents and carers right to manage their child's digital life outside of school.

Staff use of social media is covered by the Use Of Social Network Sites Policy.

Cyber-Bullying

Cyber-bullying is the use of digital technologies, particularly mobile phones and the internet, and specifically social networking sites, to deliberately upset someone else. Some features of cyber-bullying are different from other forms of bullying. These differences include:

- The invasion of home and personal space;
- The audience can be very large and reached rapidly;
- People who cyber-bully may attempt to remain anonymous;
- Cyber-bullying can take place between peers and between generations, with teachers/staff becoming victims;
- Some instances can begin unintentionally. The school community has a duty to protect all its members and provide a safe, healthy environment. Although bullying is not a specific criminal offence in the UK, there are laws that can apply in terms of harassing or threatening behaviour.

All cyber-bullying incidents will be recorded and investigated. The relevant staff will be kept informed by use of CPOMS. Steps will be taken to identify the bully, which may involve interviewing witnesses. Once the person bullying is identified, steps will be taken in line with the school's behaviour policy to modify their attitude and behaviour as well as ensuring access to any support that is required. School will advise parents of how they can protect their child from cyber-bullying and as school cannot condone the underage use of social media school may recommend that parents delete social media accounts. Incidents of cyber-bullying that are deemed serious enough may be reported to the police.

Other Areas To Consider:

Information system security

School computing systems capacity and security will be reviewed regularly.

Virus protection is updated regularly.

Security strategies will be discussed with the school's ICT technical support.

Managing filtering

The school will work with the Internet Service Provider (BTLancs) to ensure that the Lightspeed system used to protect pupils are maintained.

Whilst filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that the appropriate action can be taken.

Monitoring

Pupil use of the internet will be monitored in the first instance by shoulder surfing.

Lightspeed will create a weekly report of any inappropriate search terms used, or blocked sites that will be emailed to the ICT lead.

Any inappropriate use detected will be cross-referenced with class timetables.

Managing failures in online safety

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer or tablet. School will deal with failures in online safety in the following way:

Teacher's will minimise immediate risk to children by completing a dynamic risk assessment and acting accordingly- this might mean stopping access for one pupil or it might mean immediately stopping access for a whole class.

ICT Lead and SLT to be informed via CPOMS.

Inappropriate access to be investigated by ICT Lead to check whether it was intentional or unintentional. If intentional then sanctions to be put in place in line with Acceptable Use Policy and behaviour policy.

Any inappropriate access whether intentional or unintentional will be reported to parents by the class teacher and ICT Lead.

The school will immediately audit filtering and monitoring provision to establish if it is adequate and that its implementation is effective.

Inappropriate access to be logged in ICT Lead's file.

Lightspeed solutions to be informed.

Managing emerging technologies

The educational benefit of emerging technologies and any potential risks will be considered before it is used in school.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the GDPR.

Authorising Internet access

All staff must read and sign the 'Acceptable Use Policy' before using any school digital resource. Pupils will be asked to sign an 'Acceptable Use Policy'.

Publishing pupil's images and work

Staff and pupils using tablets, laptops, digital cameras, video recorders or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner.

Photographs that include pupils will be selected carefully.

Pupils' full names will not be used anywhere, particularly in association with photographs

Images or videos of children will only be displayed on the school website if parental consent has been given.

Where pupil's work is published the school will ensure that the child's identity is protected.

Educating parents:

Parents attention will be drawn to the school e-safety policy on the school website.

Online-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.

Twilight courses and presentations may be run by the school for parents.

Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any online-safety related concerns.

Northbrook Primary School will always promote the use of digital technologies to develop good digital citizenship. However, the digital life of a child when they are not in school ultimately remains the responsibility of their parent or carer.

Handling e-safety complaints

Complaints of internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the headteacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

ICT Acceptable Use Policy

These rules reflect the content of our school's e-Safety Policy. It is important that parents/ carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT , including the use of the internet.

- I will only use ICT in school for school purposes.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only use my class e-mail address or my own school email address when emailing.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others', details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only communicate online with people a trusted adult has approved.
- I will only open/delete m own files at my teacher's request.
- I will not attempt to download or install anything on the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT will be monitored and my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- I understand that failure to comply with the Acceptable Use policy may result in disciplinary steps being taken in line with the school's behaviour policy.

We have discussed this Acceptable Use Policy and my child _____agrees to follow the e-Safety rules and to support the safe use of ICT at Northbrook Primary School

Parent/ Carer Name (Print)……

Parent/ Carer (Signature)----------

Class …… Date :----------