



IGNITE INNOVATE INSPIRE

Digital Learning & Online Safety Policy December 2024

***'If we teach today's students how we taught yesterday's, we rob them of tomorrow.'* John Dewey**

Curriculum Vision: Why we use Digital Learning

At Monkhouse, we believe all children will be ambitious, courageous, resilient, respectful and kind so that they fulfil their unique potential and become active members of the wider global community.

Digital Learning is integral to modern day life and we strive to equip our children with the skills and confidence needed to be digitally confident and safe online. We believe that the use of technology brings enormous benefits to children and allows us to redefine their learning. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks with the intention to considerably reduce impact.

Technology is an integral part in the learning process and is used to enhance opportunities so teaching and learning is adventurous, ambitious, exciting and set in real life contexts. We aim to focus on developing curiosity, imagination, exploration and investigation, using developing technology, identifying the safe way to learn and understand the associated risks. Our teaching will provide children and the school community with the skills and knowledge to use technology appropriately and responsibly both inside and outside school.

The Digital Learning and Online Safety Policy should be read in conjunction to the Acceptable Usage Policy for pupils, staff and visitors.

Creating a safer online culture

At Monkhouse, we all rely on and benefit from the use of technology. As a school we aim to instil a safe online culture and realise how challenging it can be for home environments to ensure that their child remains safe online. We also appreciate that it is desirable to have particular measures in place to ensure that a child does not view inappropriate material from their mobile

device or from a device at home. Where we hold a responsibility in educating children within Online Safety, at Monkhouse, we demonstrate our commitment to protecting our pupils online by working with National Online Safety, which we use to educate our children and also to provide resources for all parents and carers. These resources include explanation videos, monthly newsletters and weekly guides covering a huge range of topics: all of which can be viewed within your created space. As a school, we frequently encourage all parents and carers to sign up to this free to use resource through our school portal. In maintaining this safer culture and home relationship, we will often share particular information through the parental portal to keep parents and carers informed.

Device management and Acceptable Usage Agreement

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in line with GDPR policies and practices.

In Monkhouse, where Early Years have access to a class set of iPads, KS1 children have access to shared devices across both Year 1 and 2. In KS2, we follow a 1:1 iPad scheme for our children. We recognise that the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using them:

Monkhouse Primary School does not prohibit the use of personal mobile devices on the school network (tablet or iPad). However, pupils and parents should note the following items and be aware of and agree to the terms outlined in the Pupil Acceptable Usage Policy. These examples are for clarification: they are not exclusive.

- Any mobile device must be checked for viruses and spam content before being attached to the school network.
- Mobile devices must not be used to take photographs or sound clips of any person, who is unaware of the action and who has not given their permission. Photographs/images of children should not be stored on any of these devices.
- Any use of mobile technology to intimidate, bully, harass or threaten others will be counted as an infringement of network use. This may result in disconnection from the network or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission.
- School managed iPads are added to the school management device system, where these can be tracked and restrictions added. Only age appropriate apps will be added to iPads and apps downloaded on the school account are managed centrally.
- Home iPads brought into school are encouraged to have restrictions on them from home. Children are only permitted to use apps as directed and if any inappropriate apps or content is found on the iPad this is discussed with parents and recorded suitably
- Children are made aware that they should only take photographs and record each other with express permission and not use these images other than in the way intended
- When children leave Monkhouse, iPads purchased on the school leasing scheme have all school apps and management devices wiped to ensure no data is left on the iPad

- iPads are only to be used as directed to the class teacher and all websites and apps directed to be used are appropriately checked prior to dissemination
- Apple classrooms may be used in school to monitor and direct children's use of iPads in lessons. Any screen monitoring or control is not able once the iPad leaves the school setting
- All school iPads to be added to the school management device to allow these to be tracked and these are all collected at the end of the day in labelled boxes. Any missing iPads to be tracked and parents contacted of who it is allocated to in order to see if it has been taken home in error.

We are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

Our Using images of children consent: photographs, videos, websites, mobile phones and webcams policy clearly sets out the consent from pupils, parents and staff.

- Parent's permission is sought when they enter school. They can agree to aspects of photographs being used in school and beyond. Parents can withdraw their consent at any time.
- Once children have left the establishment any photographs of them are deleted unless they have been used in school documentation where consent has been given.
- A list of consent for photographs is provided to each teacher annually and updated by the office staff where consent changes.
- At certain events, parents may take video and photographs of their child engaged in school events for their personal use. Any attempt to publish them on any social network sites or the internet is not allowed. As written in our using digital images policy.
- Only school equipment will be used for taking photographs of children which can only be used for school purposes. All images must not be stored on mobile devices but securely on the schools shared server where password access protects the images.

In our school the following statements reflect our practice in the use of various areas. As a school we also comply to GDPR procedures and follow the regulations set out regarding how we handle data and historic images of children, who are no longer a part of our school.

Jamf Mobile Device Management Systems

In order to secure device use in school, all iPads are managed under Jamf to allow for appropriate restrictions on child iPads during school hours. Profiles are assigned to ensure device use fits in line with education purposes with home apps and communication apps hidden from 8:30 am to 3:30 pm term time. This supports the safeguarding of use under school provision. Where wider use may happen at home school make parents and carers aware that they have a duty of care and responsibility to support and deal with any online issues between children so that that time is not impacted during the school day.

Impero Web Filtering Software

Impero will be used on all iPads to provide robust web filtering, ensuring compliance with *Keeping Children Safe in Education* (KCSIE) guidance. While Jamf allows us to create blocklists for specific app types, its web filtering capabilities are not sufficiently robust to safeguard students against harmful or inappropriate online content. Impero's advanced filtering system will monitor and block unsuitable websites in real-time, offering a more comprehensive safeguarding solution that aligns with statutory requirements. This layered approach ensures both app and web-based content is appropriately managed to maintain a safe digital learning environment.

Key features include:

- **Web filtering:** Restricts access to unsuitable websites and content, customisable to meet school requirements.
- **Keyword detection:** Alerts staff to potential safeguarding concerns such as cyberbullying, radicalisation, or self-harm.
- **Monitoring and reporting:** Provides detailed reports and insights into online activity, helping staff identify and address risks.
- **Compatibility:** Works across various devices and platforms.

Email

All staff and children have a secure Gmail email address and Google Drive. This is the only email they access in school or using school ICT hardware. Only official email addresses should be used to contact staff/pupils. All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.

All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security. All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy. All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Media:

The minimum age for registering for many social media sites exclude primary school pupils. These communication tools are, by default, 'blocked' through the internet filtering system for direct use in North Tyneside schools.

Although we do not allow access to social networking sites in school for children, we do understand they may use these out of school. We teach children that some sites have age restrictions for membership (e.g. Facebook age 13yr +) as well as the risks around using these sites and how to use them appropriately. Issues that relate to social networking sites such as keeping personal information safe and protecting their online identity are taught through our e safety curriculum at appropriate times throughout the year. In school, we monitor social media for any unacceptable inappropriate use by children. Information on age limits for having social media is regularly communicated to parents. If it is found a child is using a social media account

inappropriately, parents will be contacted to ensure consent has been given and where necessary the account will be reported.

Twitter and blogging may be accessed through school networks by staff through the appropriate school accounts where the use is solely for school purposes.

Mobile telephone:

Only Year 5 & 6 children are allowed to bring mobile phones into school if they walk to and from school unaccompanied. On entering the school site, all mobile phones are turned off, brought to the office and locked away until 3.30pm when they are collected by the children. We acknowledge that some children have phones where they can access the internet and we ensure that appropriate teaching and learning around the safety of using these devices to keep themselves safe.

Fitness devices and watches are permitted for children in school, however if these are paired to a mobile phone (apple watch) this is treated the same as any other mobile device and either should not be brought to school or handed to the school office.

Instant Messaging and video messaging

Children may have access to instant messenger services on their iPad. These services (WhatsApp, iMessaging) are not permitted to be used in school. Any instances of inappropriate use are recorded and dealt with in line with the AUP or in instances of bullying via our school's behaviour for learning policy

Virtual Learning Environment (VLE) / Learning Platform:

- All children have logins for Gmail. Where passwords are supplied children are taught to keep these private for security reasons. All children have gmail email addresses. Pupils may only use approved email accounts on the school system. Pupils must immediately tell a teacher if they receive an offensive email.
- Pupils also have access to an online portfolio/journal, where they hold individual login details for this through a code and/or QR code.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Email 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.
- The forwarding of chain letters is not permitted.
- As children leave the school their accounts at Monkhouse are deleted
- Internet usage and spot checks on iPads are carried by the school office

Web sites and other online publications

Pupils' full names will not be used anywhere on the school's web site, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

The website is maintained by the office staff and computing lead, this is updated regularly and audited on a termly basis to ensure this is kept up to date. However, subject leads have access to their subject's profile.

Education and Training

We believe staff and pupils need to be digitally confident and aware of the benefits that the use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

The three main areas of online safety risk that we need to be aware of and consider are:

Area of risk	Examples of risk
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising e.g. SPAM Privacy of information (data protection, identity fraud, scams, phishing) Invasive software e.g. Viruses, Trojans, Spyware Premium Rate services Online gambling
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	Illegal materials Inaccurate/bias materials Inappropriate materials Copyright and plagiarism User-generated content e.g. YouTube, Sexting
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying Contact Inappropriate emails/instant messaging/blogging Encouraging inappropriate contact

How will staff, pupils and parents be kept informed?

Staff

It is important that Staff feel prepared for Internet use and agree with the school's Acceptable Usage Policy. Staff should be given opportunities to discuss the issues and develop good teaching strategies. Staff have access to self-led CPD through National Online Safety and are made aware of the relevant computing policies and changes prior to being issued with their school Google account credentials and/or receiving school equipment for their professional use.

Parents

There may be a gap between some parents' awareness of safety issues, and the technical proficiency of their children. Therefore, the school provides information and guidance to help

bridge this gap through a variety of means, including briefings at Parents' Evenings, letters, newsletters, and the Parents' Portal and App provided via National Online Safety.

Should parents have any concerns over, or wish to seek guidance on, any aspect of Online Safety or the use of technology, they are encouraged to contact their child's teacher in the first instance. In the event of more serious issues parents and carers are invited to contact the Headteacher - Laura Baggett, the designated safeguarding leads - Laura Baggett and Carol Moulder or the Computing and Digital Learning lead - Ben Hayden. At Monkhouse, we believe that communication between home and school is vital in the establishment of good use of technology safety principles and practice.

Should parents have concerns that their child has been subjected to attempts of inappropriate online contact, they should contact the relevant Designated Safeguarding Lead as a matter of importance. Where appropriate, the DSL's will liaise with outside agencies, such as social services, the police and possibly also the CEOP (Child Exploitation and Online Protection) service, (details of which can be found at www.ceop.police.uk)

Should parents wish to discuss any other aspect of online behaviour, such as possible online gaming addiction, or concerns about the amount of time spent online, they should similarly contact any of the relevant staff as a matter of importance.

Pupils

Pupils receive frequent, planned teaching in Online Safety both as part of their Computing curriculum and in line with statutory PSHE (Life Skills) classes. Pupils are taught how to take a responsible approach to their own digital world. Theme based assemblies also contribute to the effort to raise awareness at appropriate times during the year

Through the use of materials provided by National Online Safety, all teaching and learning falls in line with the latest statutory guidance issued by the Department for Education. This includes 'Keeping Children Safe in Education (KCSiE)', 'Teaching Online Safety in Schools', 'Relationships Education, Relationships and Sex Education (RSE) and Health Education' and the 'Education for a Connected World' framework.

We ask that you note that through these sessions, the different forms of 'bullying' including 'cyber bullying' are discussed with children as part of Life Skill lessons and where to seek help if this happens to them. Although we discuss this under the term 'negative online interactions' so that children's perception of 'bullying' is not a term they undertake as a go to phrase or word. We develop clear definitions and use social stories and scenarios to identify, where an interaction may be purely down to an isolated or non-persistent event.

The Online Safety policy is regularly reviewed and approved by the governing body.

Dealing with incidents

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). **Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (See Appendix 1). Always report potential illegal content to the Internet Watch Foundation (<http://www.iwf.org.uk>). They are licensed to investigate – schools are not!

Examples of illegal offences are:

Accessing child sexual abuse images

Accessing non-photographic child sexual abuse images

Accessing criminally obscene adult content

Incitement to racial hatred

More details regarding these categories can be found on the IWF website

<http://www.iwf.org.uk>

Inappropriate use

Some examples of inappropriate incidents are listed below with suggested consequences.

Incident	Procedure and Consequences
Accidental access to inappropriate materials.	Minimise the webpage Tell a trusted adult. Enter the details in the Incident portal and report to e learning lead if necessary. Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	Inform SLT or designated computing lead Enter the details in the Incident portal. Additional awareness raising of eSafety issues and the AUP with individual child/class.
Deliberate searching for inappropriate materials.	More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. Consider parent/carer involvement.
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	Be aware that a CP concern may be raised for a child if inappropriate. See CP designated teacher for any historical / current concerns.

Any incidents should be logged through CPOMS and alerted to the Computing and Digital Learning Lead, DSL and SLT where necessary. The computing lead will monitor the CPOMS category, where contact with parents will depend on the inappropriate use. Any repeat offence will involve immediate contact with parents unless it is a matter of CP which may put the child at risk of further harm.