North Manchester Primary Federation
E-Safety Policy

Date of review	Amendments Made
13/04/18	Where there is evidence of emerging technological threats, in school or at home, we will ensure that children and parents are educated about the risks involved, reminded of legal age for accessing particular websites and apps and provide support within the home for parents to set appropriate filters. In addition to this, workshops are offered annually to parents around e-safety and how to support their children to keep safe when using technology.(Page 2)
08/05/19	The policy has been reviewed and there are no changes.
Jan 2021	Reference to remote learning policy included page 3: **The content of this report applies to children and adult's use of technology in school, at home and through remote learning (for example during national lockdowns and periods of self-isolation).**
May 2021	Reviewed – no changes.
October 2022	Updated to include reference to the updated 'Keeping Children Safe in Education' 2022. P3: Include the 4 key categories of risk P5-6: More detail around e-safety training for children, parents & staff P7: Detailed paragraph about cyber-bullying & procedures around electronic device searches
October 2023	

Contents

1. Introduction

At North Manchester Primary Federation, we wish to enrich and enhance the use of ICT and computing through various ways:

- The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.
- Use of email, mobile phones, Internet messaging and blogs all enable improved communication and facilitate the sharing of data and resources.
- Virtual Learning Environments (VLEs) provide children and/or young adults with a platform for personalised and independent learning.

Unfortunately, there are dangers associated with the Internet and emerging new technologies are highly publicised in the media. For example:

- Children might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful emails.
- Children might receive unwanted or inappropriate messages from unknown senders via email or via files sent by Bluetooth. They might also be exposed to abuse, harassment, 'sexting' or 'cyber-bullying' via email, text or instant messaging, in chat rooms or on social-networking websites, such as Facebook, Bebo, Facebook, etc.
- Reminders are always given to the children when using You Tube for educational purposes that they need to be 13 to have their own account.
- There are constant reminders to children that you need to be at least 13 to have a Facebook or Instagram account.
- Chat rooms provide cover for unscrupulous individuals to groom children.

Where there is evidence of emerging technological threats, in school or at home, we will ensure that children and parents are educated about the risks involved.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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

New technology provides a wealth of social and educational benefits, such as:

- Children are equipped with skills for the future.
- The Internet provides instant access to a wealth of up-to-date information and resources from across the world, which would not be otherwise available.
- The Internet helps to improve children's reading and research skills.
- Email, Instant Messaging and Social Networking helps to foster and develop good social and communication skills.

Thus, benefits far outweigh the risks involved so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

This E-Safety policy, written in accordance with school policy, Manchester guidelines and Keeping Children Safe in Education, focuses on each individual technology available within school and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to.

The content of this policy applies to children and adult's use of technology in school, at home and through remote learning.

Staff at North Manchester Primary Federation are aware that the procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into the school and that this policy will not remain static. It may be that staff and children might wish to use an emerging technology for which there are currently no procedures in place. It is therefore advisable to state that the use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.

2. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.
In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

3. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents on the school website.

Online safety will also be covered during various workshops throughout the academic year.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access
- Safe online practices at home, including parental settings, filters and appropriate websites & apps for age

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the phase leader who will seek support from a Designated Safeguarding Lead or Computing Lead.

Concerns or queries about this policy can be raised with any member of staff or the Head of School.

4. Training staff on online safety

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training throughout an academic year as part of safeguarding training, as well as being given relevant updates as required (for example through emails, minutes and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The Designated Safeguarding Leads in school will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals.

Volunteers will receive appropriate training and updates, if applicable.

5. Cyber-bullying

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 1 person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

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 PSHE education, 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.

Examining electronic devices

The Executive Headteacher, Head of School, or any member of staff authorised to do so by the Executive headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from Executive Headteacher or Head of School
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to Executive Headteacher or Head of School to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6. Shared school network protocols

This section includes what users must and must not do when using a PC / laptop/tablet/iPad connected to the school network.

- Users must access the school network using their own logins and passwords. These must not be disclosed or shared **UNDER ANY CIRCUMSTANCES.**
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- Software should not be installed, nor programmes downloaded from the Internet, without prior permission from the Computing Lead or Technician managing the network.
- Removable media (e.g. pen drives / memory sticks) **MUST NOT** be used, unless it is an encrypted memory stick that has been authorised by the Computing lead or technician. Files should be saved on laptops or towers or emailed to an address in order to reduce the number of viruses.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').
- Machines must be 'logged off' AND 'shut down' correctly after use.

N.B. The wireless network must be encrypted to prevent outsiders from being able to access it. Passwords must be encrypted to prevent outsiders from being able to access it.

7. Internet and email protocols

- All users (staff, children, visitors, students on placement) must sign an Acceptable Use Agreement before access to the Internet and email is permitted in the establishment.
- Parental or carer consent is *requested** in order for children to be allowed to use the Internet or email.
- Users must access the Internet and email using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's email account.
- The Internet and email must only be used for professional and educational purposes. For children the internet for research and the supervised use of the school email accounts **ARE ACCEPTABLE.** Strict supervision of Google Images by an adult for research purposes is also **ACCEPTABLE.** For Staff, the downloading of YouTube videos and Google Images for delivery of lessons **IS ACCEPTABLE,** as long as the use is for educational purposes.
- For children: the use of social networking sites and unsupervised use of the internet **IS NOT ACCEPTABLE.**
  For Staff: the downloading of YouTube videos for social use, use of non-school email accounts and personal use (for example social networking sites and

online banking) **IS NOT ACCEPTABLE.**

- Children must be supervised at all times when using the Internet and email.
- Procedures for Safe Internet use and sanctions applicable if rules are broken will be clearly displayed beside every computer with access to the Internet. Sanctions are noted before the concluding statement.
- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the Executive Headteacher or Head of School and a note of the offending website address (URL) taken so that it can be blocked by the ICT technician. If this event happens, staff are to tell children to shut the lid of the ipad or net book and tell an adult immediately.
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly.
- Internet and email use will be monitored regularly in accordance with the Data Protection Act.
- Email addresses assigned to individuals will not be easily recognisable or told to others.
- Users, both adults and children, must not disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions are noted before the concluding statement (Page 9) and will be imposed on any users who break this code.
- All emails sent from a school email account will carry a standard disclaimer disassociating the school and the Local Authority with the views expressed therein.
- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, which are noted before the concluding statement, (Page 9) will be imposed on any users who break this code.
- If users are bullied, or offensive emails are received, this must be reported immediately to the Executive or Associate Head teacher or member of the senior leadership team if they are unavailable. Emails received should not be deleted, but kept for investigation purposes.
- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.
- All email attachments must first be scanned before they can be opened.
- Users must seek permission before downloading any files from the Internet.
- All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet.

8. Instant messaging, chat and weblog protocols

- The use of Instant Messaging is not permitted.
- Use of Social Networking websites, such as Bebo, MySpace, Facebook, Moshin Monsters, Club Penguin and Piczo is not permitted. *(This list is not exhaustive)*
- Children and staff must not access public or unregulated chat rooms.
- Use of blogs is permitted for educational purposes. This will be supervised and children will be reminded of the safe practices and behaviours to adopt when posting material, as well as the need to adopt a formal and polite tone at all times. Posts and comments will be checked and authorised before they go live on the website.
- The school will be able to blog and comment on each other's through safe practice of allowed blog sites and the school website.

9. Taking photos, videos and web cam protocols

- Consent is obtained from parents and carers as to whether a child can have their photograph or video taken and where this can be uploaded (in school, website, social media etc) Staff across the school will be aware of who can have images taken in their class and who cannot and where these are shared. The school office team have a whole school list where staff can check if they are unsure.
- Adults should not use their own devices to take images as per our Safeguarding Policy.
- Photographs or video footage will be downloaded immediately and saved into a designated folder. Any photographs or video footage stored must be deleted immediately once no longer needed.
- Children should not have their mobile phones in school. Watches which can take photographs or videos are also not permitted in school.
- Parents will be reminded at events (assemblies, shows) that taking images on their mobiles is not permitted as they do not have consent from all parties involved. Any parent seen recording will be asked to stop and delete images they have recorded or taken so far.
- Children MUST not accept files sent via Bluetooth to their mobile phones by an unknown individual. If they do, and the content received is upsetting or makes them feel uncomfortable, they should pass this on to a trusted adult straightaway.
- Video conferencing equipment and webcams must be switched off (disconnected) when not in use and the camera turned to face the wall.
- Webcams must not be used for personal communication and should only be used with an adult present.
- Children and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be

appropriate to the audience and situation.

10. Safety of the school website

The Computing Lead, along with the Executive Head teacher and Head of School are responsible for the content and images uploaded onto the school website.

- Copyright and intellectual property rights must be respected.
- Permission must be obtained from parents or carers before any images of children can be uploaded onto the school website.
- Names must not be used to identify individuals portrayed in images uploaded onto the school website. Similarly, if a child or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.
- When photographs to be used on the website are saved, names of individuals portrayed therein should not be used as file names.
- The guestbook, public notice board and forums must be monitored at least three times a week to check that no personal information or inappropriate or offensive material has been posted. Material that is classed to be offensive will be reported immediately to the head teacher and a CPOMs log will be completed. The IP address should be noted, in case further action is required. These files will be kept as evidence.
- The school website should be subject to weekly checks to ensure that no material has been inadvertently posted, which might put children or staff at risk.

11. Mobile phones and Personal Digital Assistants (PDAs)

Staff should not use their mobile phone during lesson times and if they are around the children.

- ***What must children and staff in your school do if they receive unwanted, unsavoury or hurtful calls, text messages or files sent via Bluetooth?***
  This should be reported, whilst any such messages or files received should be kept for investigation purposes and not replied to. In the case of Bluetooth, individuals have the option to refuse a file. If the person is unknown to them, they should be advised not to accept it. If they inadvertently accept inappropriate content, or do so out of curiosity, they must not be afraid to report this and any files should be retained and not deleted.

12. Games Consoles

At the North Manchester Primary Federation, it has been decided that these are not appropriate for children to bring into school. Not only might their presence lead to instances of theft, but as children can also connect to the Internet and play against other people online, they represent the same dangers as public chat rooms.

13. Breach of NMPF protocols

Cases of misuse will be considered on an individual basis by the Head of School or Computing Lead and sanctions agreed and imposed to 'fit the crime.'

Staff members & volunteers

The adult in question will be called to discuss their breach with the Head of School or Computing Lead. From this point, it will be determined whether the next course of action is formal or informal. Advice and guidance from HR will be sought.

Pupils

Letters will be sent home to parents or carers. A log on CPOMs will be completed and kept on the child's file.
Users may be suspended from using the school's computers, Internet or email, etc. for example, for a period of ONE week initially, with further sanctions if this continues.
Details may be passed on to the police in more serious cases.
Legal action may be taken in extreme circumstances.

> ***Serious misuse, such as bullying, sexting, harassment, language of an inappropriate nature, including homophobic, bi-phobic and transphobic language, as well as racism will result in an immediate suspension from the use of all internet access whilst an investigation takes place.****

14. Monitoring arrangements

This policy is reviewed and approved by the Executive Headteacher and full governing body annually, taking into account recent government guidance.

15. Links with other policies

11. Links with other Policies

This E-Safety Policy is linked to the following policies:

- Safeguarding Policy
- Behaviour Policy

Appendices

- **Acceptable Use Agreement (AUP) for Staff**
- **Acceptable Use Agreement (AUP) for Pupils / Young adults**
- **Acceptable Use Agreement (AUP) for Guest Users**

Staff ICT Acceptable Use Statement

Staff should sign and have a copy of an Acceptable ICT Use Agreement. In signing, staff accept that the school can monitor network and Internet use to help ensure staff and pupil safety. The school's e-safety policy should be consulted for further information and clarification.

1. The information and communication technology and related systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
2. I will ensure that my information systems use will always be compatible with my professional role.
3. I understand that school information systems may not be used for private purposes, without specific permission from the Executive headteacher or Head of School.
4. I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
5. I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
6. I will not install any software or hardware without permission.
7. I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
8. I will respect copyright and intellectual property rights.
9. I will report any incidents of concern regarding children's safety to the school e-safety co-ordinator and record on CPOMS for the attention of the Designated Safeguarding Leads
10. I will ensure that any electronic communications with pupils are compatible with my professional role.
11. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Technology and Communication Acceptable Use Statement.

Signed: …… Date: …….....

Accepted for school by: …… Date: …….....

Name _____

Year Group _____

Please tick your preferred statement.

- ☐ I **give consent** to photos/videos being used for educational purposes **both in and out of school**, including the website

- ☐ I **do not give** consent to photos/videos being used for educational purposes.

- ☐ I **give consent for photos and videos** to be on displays, newsletters and brochures, but **NOT** on the website.

Signed: _____

Date: _____

Foundation Stage & Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Pupil, Child, Parent and teacher sign this on the Home School Agreement

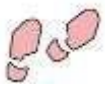
Key Stage 2

Think then Click

These rules help us to stay safe on the Internet

- We ask permission before using the Internet.
- We only use websites that are safe.

- We tell an adult if we see anything we are uncomfortable with and shut the lid of the net book or i pad.
- We only e-mail people an adult has approved.



- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Pupil, Child, Parent and teacher sign this on the Home School Agreement

Visitor ICT Acceptable Use Statement

Visitors are requested to sign and have a copy of an Acceptable ICT Use Agreement. In signing, you accept that the school can monitor network and Internet use to help ensure staff and pupil safety. The school's e-safety policy should be consulted for further information and clarification.

1. The information and communication technology and related systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
2. I will ensure that my information systems use will always be compatible with my professional role.
3. I understand that school information systems may not be used for private purposes, without specific permission from the Executive Headteacher or Head of School.
4. I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
5. I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
6. I will not install any software or hardware.
7. I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
8. I will respect copyright and intellectual property rights.
9. I will report any incidents of concern regarding children's safety to the school Desginated Safeguarding Leads.
10. I will also log details in e- safety log book located in the research room/ICT room if any issues arise.
11. I will ensure that any electronic communications with pupils are compatible with my professional role.
12. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Technology and Communication Acceptable Use Statement.

Signed: …… Date: ……..

Accepted for school by: ……. Date: ……..