North Manchester Primary Federation

Crumpsall Lane Primary School
Crumpsall Lane
Crumpsall
Manchester
M8 5SR
Tel: 0161 740 3741
Email: admin@crumpsall.manchester.sch.uk

Crab Lane Primary School
Crab Lane
Higher Blackley
Manchester
M9 8NB
Tel: 0161 740 2851
Email: admin@crablane.manchester.sch.uk

E-Safety Policy
Jan 2021

Date	Amendment 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.

Introductory Statement

At the 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 MySpace, 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, 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.

However, 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, as well as

Manchester guidelines, focuses on each individual technology available within the

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 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).

Cyber Bullying

Bullying is usually part of a pattern of behaviour rather than an isolated incident. However, if an individual considers themselves to have been bullied, this may have a negative impact on their emotional well-being, which can perpetuate the fear of a further perceived or real incident. Any reported incident must be taken seriously.

Cyberbullying can include email and internet chat room misuse, mobile threats by text or calls, misuse of associated technology, i.e. camera/video facilities, etc.

North Manchester Primary Federation recognises that the production and distribution of sexting images involving anyone under the age of 18 is illegal and needs very careful management of all those involved. This will be reported to the Designated Safeguarding Lead (DSL) and the device will be confiscated. If relevant, this will be reported to Children's Services and the police. For further advice, contact Professional Online Safety Helpline. (0844 381 4772)

Homophobic, bi-phobic and transphobic language and online bullying both on school computers and outside of school will not be tolerated and the same sanctions will apply to this type of bullying as in the classroom.

Procedures for Use of a Shared School Network

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 ICT Leader 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 ICT leader 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'). The e safety committee will do regular checks to ensure that this is being done.

- 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.)

Procedures for Use of the Internet and Email

- 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 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 persons responsible for E-Safety (Malcolm Jones, Pat Adams) 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.

Procedures for Use of Instant Messaging (IM), Chat and Weblogs

- 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.

- 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.

Procedures for Use of Cameras, Video Equipment and Webcams

- **Permission must be obtained from a child's parent or carer before photographs or video footage can be taken.**

- Photographs or video footage will be downloaded immediately and saved into a designated folder. This will be 'password-protected' and accessible only to authorised members of staff.

- Any photographs or video footage stored **must** be deleted immediately once no longer needed.

- Any adult using their own camera, video recorder or camera phone during a trip or visit **must** transfer and save images and video footage into a 'password-protected' folder onto a school computer immediately upon their return.

- 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.

- In EYFS, images are taken to add evidence to the child's Learning Journey. Staff using this need to ensure that they are aware of children that can not be photographed for safeguarding purposes. Staff must only take photos of the individual child. When referencing the whole class or groups of children staff must add a comment without a photo.

Procedures to ensure safety of the school's website

- The school should have a designated member of staff who is responsible for approving all content and images to be uploaded onto its website prior to it being published. (Mrs. Hatton and Mr. Jones)

- 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.

- **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 noticeboard and forums must be monitored at least three times a week (Mrs. Hatton and Mr. Jones) 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.

Procedures for using mobile phones and Personal Digital Assistants (PDAs)

- Staff are required to switch mobile phones off during lesson times.

- The taking of still pictures or video footage without the subject's permission is not ethical, so permission needs to be obtained.

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.

Procedures for using wireless games consoles and iPods.

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.

Sanctions to be imposed if procedures are not followed

- Letters will be sent home to parents or carers. A log on CPOMs will be completed and kept on the child's file.
- Users will be suspended from using the school's computers, Internet or email, etc. 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.*****

Cases of misuse will be considered on an individual basis by a named person (s) and sanctions agreed and imposed to 'fit the crime.'

Concluding Statement

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.

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 headteacher.
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 Coordinator (Mr. Jones and Mr Chippindall) or the Designated Child Protection Coordinator. (Ms. Adams and Mr. Hughes)
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

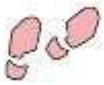
These rules help us to stay safe on the Internet

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.

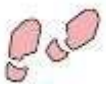
Pupil, Child, Parent and teacher sign this on the Home School Agreement

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 Headteacher.
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 e-Safety Coordinator (Mr. Jones and Mr Chippindall) or the Designated Child Protection Coordinator (Ms Adams or Mr Hughes). I will also log details in e-safety log book located in the research room/ICT room if any issues arise.
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: …….....