Online safety Policy 2020
St. Michael in the Hamlet Primary School

1. Context

We live in a digital age where technology is playing an ever increasing part in our lives and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with the school are able to use technology in a safe and responsible manner. It is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way, so that risks can be significantly reduced and users can be taught to manage them effectively.

2. Writing and reviewing the Online safety policy

The Online safety Policy is part of the School Development Plan and will operate in conjunction with other school policies including those for the RRSA, Safeguarding, PHSE and Anti-Bullying and will be displayed on the school website, where further guidance can be accessed. The Online safety policy will be reviewed annually by the SMT using relevant guidance such as the laptop/other hand held devices – responsible use policy; Responding to incidents of Misuse (Appendix 1). The Policy will be monitored by the Safeguarding and Computing Coordinator.

Our Online safety policy has been written by the school, and has been formulated using guidance from government and Liverpool City Council's Acceptable Use Code of Practice.

Consultation with the whole school community will take place through:

- School website
- School Council /safety cadet Meetings
- Staff Meetings

This Online safety Policy approval by the Governing body pending:	October 2020
The implementation of this Online safety policy will be monitored by the:	SMT
Monitoring will take place:	Annually
The Online safety policy will be reviewed annually. The next anticipated review date will be:	July 2021
Should a serious Online safety incidents take place, the following external persons/ agencies should be informed:	LA and/or police

2. Teaching and learning

2.1. Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality online access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2. Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable 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.

2.3. Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. Managing Internet Access

3.1. Information system security

- School ICT systems capacity and security will be reviewed regularly and informed by Liverpool City Council.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

3.2. E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- 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.
- The forwarding of chain letters is not permitted.

3.3. Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4. Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, Twitter or Blogs, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

3.5. Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

- The use of such systems by teaching staff should be compatible only with their professional role (User Code of Conduct for ICT – Appendix 2).

3.6. Managing filtering

- The school will work with the Local Authority and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the ICT Technician and logged in the Online safety log book located in the school office.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7. Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Videoconferencing will be appropriately supervised for the pupils' age.

3.8. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

3.9. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- All school staff will ensure that:
    - Care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
    - Personal data is used or processed on only secure password protected computers and other devices and that these devices are properly "logged-off" at the end of any session in which they are using personal data.
    - Data is transferred securely using encryption and secure password protected devices and email solutions.
    - When personal data is stored on any portable computer system, USB stick or any other removable media the data must be encrypted and password protected.

4. Policy Decisions

4.1. Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' (see Appendix 2) before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form at the start of the academic year.

4.2. Assessing risks

- 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. Neither the school nor Liverpool City Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the Online safety policy is adequate and that its implementation is effective.

4.3. Responding to Incidents of Misuse

- Responding to incidents of misuse flowchart (Appendix 1).
- Any complaint about staff misuse must be referred to the Head Teacher.

- Complaints of Internet misuse will be dealt with by a senior member of staff. 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.
- Discussions will be held with the Police-Youth Crime to establish procedures for handling potentially illegal issues.

5. Communications Policy

5.1. Digital Communication

- When using communication technologies the school ensures the following good practice:
- The official school email service is regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, on school business or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, pupils or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Pupils at Key Stage 1 and Key Stage 2 can be provided with individual, class and group school email addresses, using the tocomail system, for educational use.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also 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.
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

5.2. Introducing the Online safety policy to pupils

- Online safety rules will be discussed with the pupils throughout the school year.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will be taught at least one hour of discrete online safety each term however more opportunities to discuss Online safety will be accessible throughout the school year.

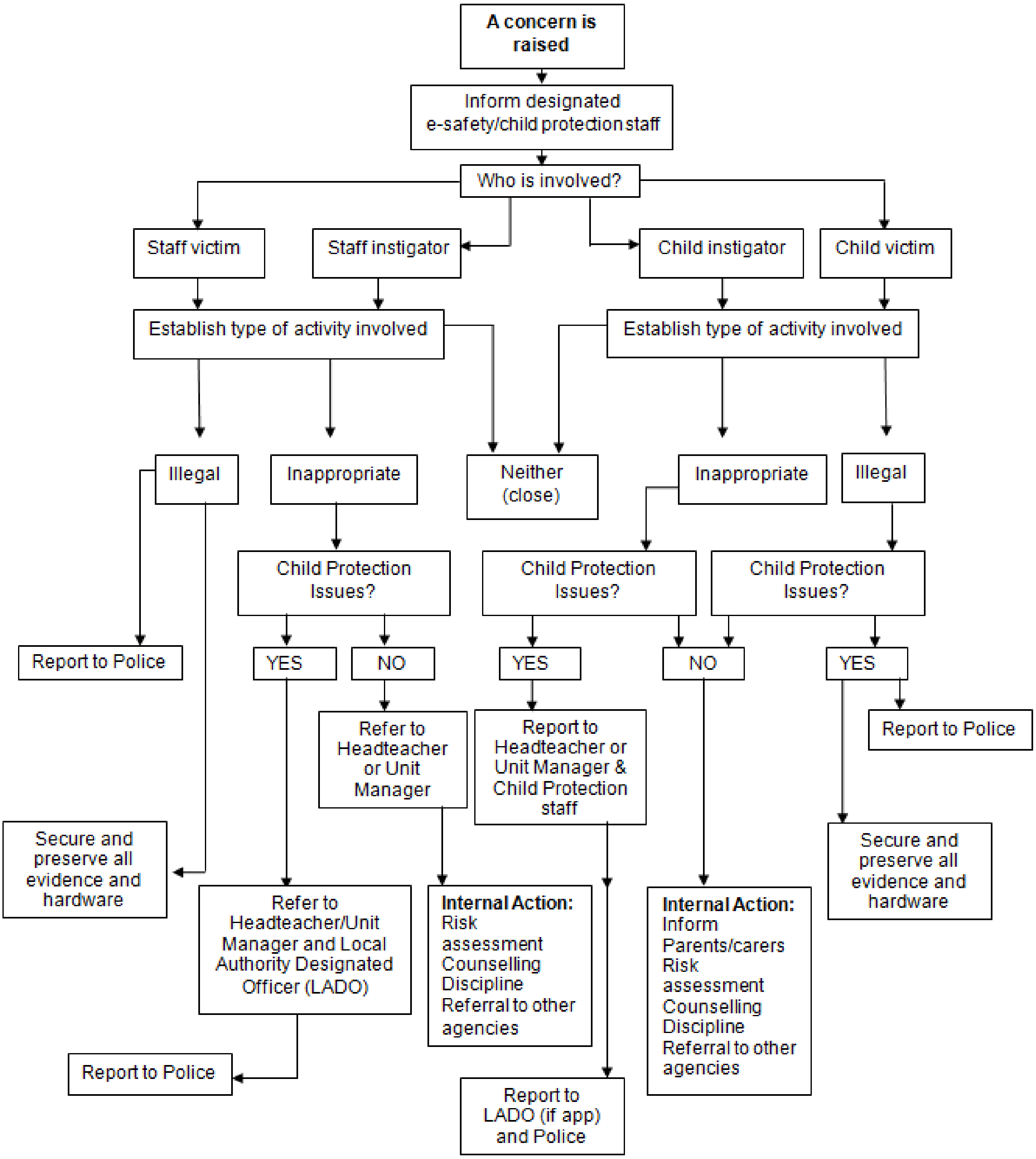
5.3. Staff and the Online safety policy

- All staff will be given the School Online safety policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff must sign an Acceptable Use policy which clearly states what is acceptable.
- The user code of conduct for ICT (Appendix 2) forms the basis of the school's expected behaviours regarding the use of technology and any infringements of the code of conduct will lead to disciplinary action against the perpetrator(s).

5.4. Enlisting parents' support

- Parents' attention will be drawn to the School Online safety policy in newsletters, the school brochure and on the school Web site.
- Parents will have the opportunity to attend an 'Online Safety Presentation'.

Appendix 1 - Responding to Incidents of Misuse – Flow Chart


A concern is raised
Inform designated e-safety/child protection staff
Who is involved?
Staff victim
Staff instigator
Child instigator
Child victim
Establish type of activity involved
Establish type of activity involved
Illegal
Inappropriate
Neither (close)
Inappropriate
Illegal
Child Protection Issues?
Child Protection Issues?
Child Protection Issues?
Report to Police
YES
NO
YES
NO
YES
Refer to Headteacher or Unit Manager
Report to Headteacher or Unit Manager & Child Protection staff
Report to Police
Secure and preserve all evidence and hardware
Refer to Headteacher/Unit Manager and Local Authority Designated Officer (LADO)
Internal Action: Risk assessment Counselling Discipline Referral to other agencies
Internal Action: Inform Parents/carers Risk assessment Counselling Discipline Referral to other agencies
Secure and preserve all evidence and hardware
Report to Police
Report to LADO (if app) and Police

All incidents will be recorded and reported to the relevant parties and organisations.

Appendix 2 – User Code of Conduct for ICT

To ensure that all members of staff and Governors are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. All staff should consult the school's Online safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras, email and social networking sites and that ICT use may also include personal ICT devices when used for school business.
- I understand that mobile phones and other personal ICT devices may only be accessed for private use during breaks or and not during scheduled working hours.
- I understand that school information systems may not be used for private purposes without specific permission from the head teacher.
- I understand that use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Online safety Coordinator, the Designated Child Protection Coordinator or Head teacher.
- I will promote Online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete 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 accept the User Code of Conduct for ICT.

Signed: .... Capitals: .... Date: ....