Maple Primary School
Policy for eSafety

January 2019

This policy is based on guidance from The Hertfordshire Safeguarding Children Board. (HSCB)

Reviewed & updated January 2019

Contents

Introduction

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

Information and Communications Technology covers a wide range of resources including; web based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include (but not exclusively):

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Online Gaming
- Internet connected smartphones and mobile devices

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements.

At Maple Primary School, we understand the responsibility to educate pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. This is done through Computing and PHSE sessions.

Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, iPads, webcams, Interactive Displays, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, iPads, mobile phones, and other mobile devices.

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The front of this document shows the named eSafety co-ordinator and Computing Subject Leader. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE.

eSafety skills development for staff

- Maple staff receive regular information and training on eSafety issues in the form of staff meetings and online resources.
- New staff receive information on the school's Acceptable Use Policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see attached flowcharts).
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas (Computing and PSHE curriculum).
- All staff have eSafety reminder/top tips posters.

Managing the school eSafety messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The eSafety policy and acceptable use policy will be introduced to the pupils at the start of each school year.
- eSafety posters will be prominently displayed. Including posters designed by pupils in the school.
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in Computing/PHSE lessons (See Computing Scheme of work, Shared Computing Folder for links and resources).
- The school provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright, respecting other people's information, the safe use of images and other important areas through discussion, modelling and appropriate activities. Children know which sites the can use for image searches.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.
- There is a focus in KS2 PHSE lessons about the acceptable and appropriate use of social media.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. All staff are expected to have secure passwords which are not shared. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's eSafety Policy.
- All staff are provided with an individual network and staff email account. As well as this, select staff are provided with an email account for Subject Co-ordination to facilitate easy handover of information when Co-ordinator roles are periodically reassigned. Staff also have individual logins for online planning websites and educational systems.
- All pupils are provided with an individual network username and shared class password.
- Pupils at Maple have individual logins for certain resources online for use at home as part of homework or as part of the school day. These passwords are shared with the parents who are expected to support them in logging in to these online resources at home.
- Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others unless under the instruction of staff as part of their education at Maple.
- If a member of staff believes any of their accounts may have been compromised or someone else has become aware of their passwords this will be reported to the Computing Subject Leader or IT Technicians.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS systems including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. In addition to this, staff must make sure that any paperwork with their personal passwords written on, must be kept private.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008) Although this organisation was closed in 2011, its information is still relevant.

Local Authority guidance documents can be found at:

HGfL: School Admin: School Office: Data Protection and Freedom of Information

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the Headteacher.
- School Data can be access by authorised staff using provided computing devices such as laptops and tablets. Select staff also have access to school data using secure Login Anywhere Remote Access services provided by the school.

Managing the Internet

All use of the **Hertfordshire Grid for Learning** (HGfL) is logged and these are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- Students will have supervised access to Internet resources through the school's fixed and mobile internet technologies.
- Staff will preview any recommended sites before use. Sites are saved onto shared resources area for the children to safely access.
- Image searches are discouraged when working with pupils and for pupils to use image searches without guidance.
- When Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. Parents will be advised to recheck these sites and supervise this work. Parents are encouraged to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded.
- School internet filtering is controlled through the LA's web filtering service.
- Maple Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2016, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the eSafety Co-ordinator. These actions reinforced with the children from Foundation stage onwards.
- It is the responsibility of the school, by delegation to the Network Manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school devices.
- Pupils and Staff are advised to not bring in personal removable media. It is not the school's responsibility nor the network managers to install or maintain virus protection on personal systems. If pupils wish to hand in work on removable media it must be given to the IT technician, ICT Subject Leader or the Class Teacher for a safety check first.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the relevant IT Technician. Staff are aware of the need to discuss any software and online resource requests with the IT staff.
- If there are any issues related to viruses or anti-virus software, an appropriate IT Technician should be informed immediately so this can be escalated to the relevant level of support as necessary.

Managing other web technology

Other web technology - including social networking sites

- At present, the school endeavours to deny access to social networking sites to pupils within school through the HGFL. Selected staff computers and mobile devices are able to access some social networking technologies for professional use.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location. This is reinforced to children throughout the school.
- Pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. This is a particular focus in KS2 with the rise in popularity of various social media platforms.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post.
- Our pupils are asked to report any incidents of cyberbullying to the school.
- Staff may only use blogs, wikis or similar platforms following discussion with the Computing Subject Leader and these are to be setup by the IT Team. These platforms may enable communication between pupils and teachers can in the course of marking and assessing classwork.
- Staff uploading to any school social media platforms understand that they must not have children's names relating to photographs. This is the same with images placed on the website.

Social Media

- Maple school uses some select Social Media platforms to share classwork and activities publicly. It is responsible of each class teacher to ensure these posts are in accordance with the e-Safety Policy. The ICT Team (Coordinator and Technicians should will periodically review all postings on these technologies and monitors responses from others).

- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.

- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning. Emerging technologies will be examined for educational benefit and risk assessed before use in school is allowed. Maple School manages the use of these systems in the following ways so that users access them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices – including smart watches, for personal use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using a personal device or account.
- KS2 year groups are allowed to bring personal mobile devices including fitness wearables (Year 5&6 phones and smartphones), but not internet connected smart watches - to school. However mobile devices must be handed to the class teacher at the start of the school day. They must not use them for personal purposes within lesson time. At all times the device must be switched off when on the school site.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate messages between any members of the school community is not allowed.
- If a member of staff uses a personal device, such as a mobile phone – when on a trip – the photographs must be immediately deleted after use and only with the permission of the Headteacher. However, all staff should ensure that these devices do not place photographs or school data on any cloud based services. Staff should consult with the ICT Technicians to ensure this is the case.

School provided Mobile devices (including phones)

- The sending of inappropriate messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides a laptop or mobile device for staff, this device may be used to conduct school business outside of school.

Managing email

The use of email is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. We recognise that pupils need to understand how to compose an email in relation to their age and good 'netiquette'.

- The school gives all staff their own email account to use for all school business.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced.
- Under no circumstances should staff contact pupils, parents or conduct any school business using school email addresses unless with the permission of the Headteacher.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- When appropriate, staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account.
- Pupils may only use school approved email accounts on the school network and only under direct teacher supervision for educational purposes.
- Pupils are introduced to email as part of the Computing Scheme of Work.
- KS2 pupils have their own individual school issued email accounts. These are provided for use in class computing lessons directly relating to email use. These accounts are deactivated when not in use.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the eSafety coordinator/Headteacher if they receive an offensive e-mail.

Safe Use of Images

Staff must be aware of the potential risks of photography and filming. This includes:

- Understanding children may be identifiable when a photography is shared with personal information.
- The risks associated when photographs of children are shared on websites and in publications.
- Inappropriate photographs and video recordings of children.
- Inappropriate use, adaptation and copying of images.

Taking of Images and Film

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal electronic equipment, such as mobile phones and cameras, to record images of pupils. However with the express permission of the Headteacher, images can be taken using personal mobile devices provided they are used for purpose of school related business and are deleted immediately once used.
- The school will not use children's names in photograph captions.
- Only images of children in appropriate clothing will be taken to reduce the risk of inappropriate use.
- Images containing children and staff should not be stored on unencrypted portable media such as laptops, memory sticks and mobile devices.
- Pupils are not permitted to use personal electronic equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

Consent of adults who work at the school

- Permission to use images of all staff who work at the school is sought on induction.

Publishing pupil's images

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's images in the following ways:

- on the school website and social media.
- in the school prospectus and other printed publications that the school may produce for promotional purposes.
- recorded/transmitted on a video or webcam.
- in display material that may be used in the school's communal areas.
- in display material that may be used in external areas, i.e. exhibition promoting the school.
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using electronic or non-electronic methods)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues. Parents/carers may withdraw permission, in writing, at any time.

- Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.
- Before posting student work on the Internet, a check needs to be made to ensure that a pupils personal information is not included.
- Only the Web Manager has authority to upload to the site.

Storage of Images

- Images/films of children are stored on the school's network only.

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff. Select images maybe be made available to pupils within the confines of the school network for the use in school work only.
- All staff have the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Webcams and Video Conferencing

- Maple will not use publicly accessible webcams in school.
- If video conferencing were to take place, permission is sought from parents and carers if their children are to be involved.
- All pupils will be supervised by a member of staff when using webcams or video conferencing.

Misuse and Infringements – Complaints

Complaints relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the **Hertfordshire Flowcharts for Managing an eSafety Incident** should be followed (see appendix).

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence (see flowchart), with possible sanctions applied.
- Users are made aware of sanctions relating to the misuse or misconduct by discussing the Acceptable Use Policy at staff meetings, or with the pupils in the class.
- Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.
However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school (or when required).
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain.
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
    - Information and celebration evenings
    - Bi-annual eSafety meetings for parents.
    - Posters
    - Website information
    - Newsletter items

Writing and Reviewing this Policy

Staff and pupil involvement in policy creation

- Staff and pupils have been involved in making/reviewing the eSafety policy through staff meetings and school council meetings.

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

The date this policy has been read, amended and approved by the staff, the Headteacher and Governors is stated on the cover of this document.

Maple School
Acceptable Use Agreement:
Staff, Governors and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of Maple daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the eSafety coordinator.

- I will only use the school's email / internet / intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my personal information, such as mobile phone number and email address to pupils.
- I will only use the approved, secure email system(s) for school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the Headteacher and Computing coordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes online with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's eSafety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …….…….…… Date ……

Full Name …….....(printed)

Job title . . . . . .

Maple School

Acceptable Use Policy – Key Stage 2

Rules for Responsible Internet Us - Think then Click

The school has computers and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others. These e-Safety Rules help to protect pupils and the school.

- I will only access the system with my own login and password, which I will keep secret.
- I will not access other people's files.
- I will only use for school computers and mobile devices for work and homework.
- I will not bring in flash drives (memory sticks) or CD's from outside school, unless I have been given permission.
- I will ask permission from a member of staff before using the internet.
- I will immediately tell an adult if I see anything I am uncomfortable with.
- Any messages I send and receive from others will be polite and responsible.
- I will not give my details, like my home address or telephone number, or arrange to meet someone.
- I will report any unpleasant material or messages sent to me to my teacher. I understand my report would be confidential and would help protect other pupils and myself.
- I will not attempt to access any social media sites.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I intentionally break these rules, then my access to the Internet may be denied.
- Any mobile devices that I have permission to bring with me to school will not be used and be turned off on school grounds.

Maple School

eSafety Rules

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the eSafety Rules have been understood and agreed.

Pupil:	***Year group:***

Pupil's Agreement

- I have read and I understand the school eSafety Rules.
- I will use the computer network, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Please complete, sign and return to your child's teacher no later than **Friday 14th December**

Maple School

Acceptable Use Policy – Key Stage 1

Rules for Responsible Internet Use

Think then Click

The school has computers and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others. These e-Safety Rules help to protect pupils and the school.

Think before you click

- I will only use the internet when an adult is with me.
- I can click on the buttons or links when I know what they do.

- I can search the Internet with an adult.
- I will always ask if I get lost on the Internet.
- I will only go on websites I have been told to go on.

- I will tell an adult if I see something I do not like.

Maple School

eSafety Rules

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the eSafety Rules have been understood and agreed.

Pupil:	***Year group:***

Pupil's Agreement

- I have read the Acceptable Use Policy with my child and they understand the school eSafety Rules.
- My child understands that they must use the computer network, Internet access and other new technologies in a responsible way at all times.
- My child understands that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Internet Access

I have read and understood the school eSafety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

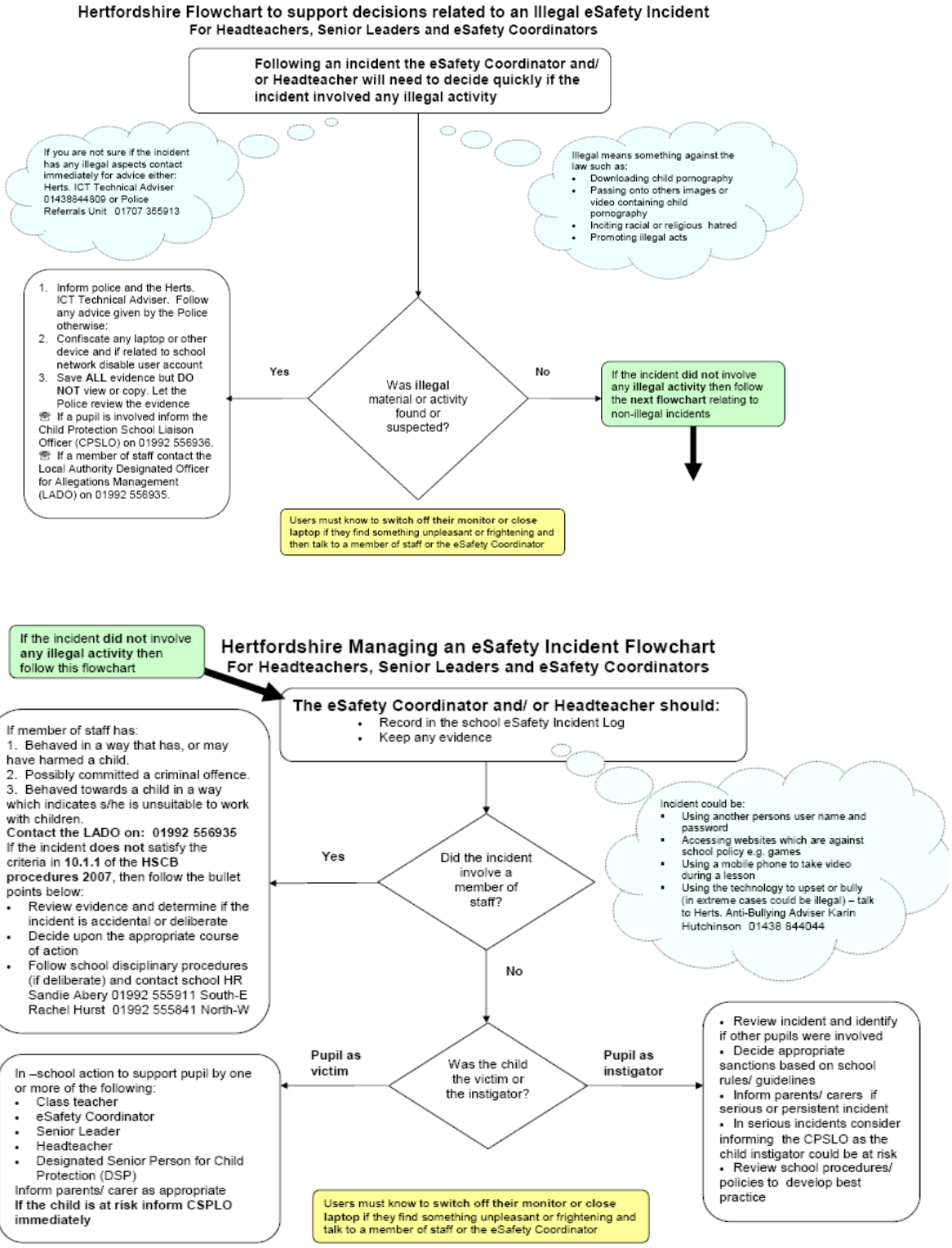
I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Please complete, sign and return to your child's teacher no later than **Friday 14th December**

Flowcharts for Managing an eSafety Incident



Maple Primary School
eSafety Incident Log

Details of **ALL eSafety incidents** to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 2018
An Act to make provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Regulation of Investigatory Powers Act 2016
An Act to make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.

Human Rights Act 1998
An Act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights; to make provision with respect to holders of certain judicial offices who become judges of the European Court of Human Rights; and for connected purposes.

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
For more information
www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Policy Review

This policy is next up for review by January 2020 and will be reviewed every year.