Owner	**Mr Story**
Date Updated	**September 2016**
Review Date	**September 2017**
Audience	**All Staff**

E-Safety Policy

Introduction

The School's appointed E-Safety Coordinator is: Chris Story.
Our E-Safety Policy has been written by the school and was agreed by the teaching staff in: September 2016
The Policy was approved by governors in: September 2016
The E-Safety Policy will be reviewed annually. This policy will next be reviewed in: September 2016

This policy relates to the following DfE Statutory Guidance:
- Keeping Children Safe in Education (September, 2016)
- The Prevent duty for schools and childcare providers (August 2015)

This policy should be read in conjunction with:
- Harrow Gate Primary Academy Safeguarding Policy
- Harrow Gate Primary Academy Child Protection Policy
- Harrow Gate Primary Academy Behaviour Policy
- Harrow Gate Primary Academy Mobile Phones Policy
- Harrow Gate Primary Academy Peer-to-Peer Abuse Policy
- Harrow Gate Primary Academy Data Protection Policy

Preamble:
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 our 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:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

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 (13 years in most cases).

At *Harrow Gate Primary Academy,* we understand the responsibility to educate our 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.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in

media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Good Habits

We aim to ensure our children are confident and most importantly safe users of technology. E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of E-Safety policy in both administration and curriculum, including secure, robust school network design and use.
- Safe and secure broadband from our provider (OneIT) including the effective management of content filtering.

E-Safety Curriculum

Ensuring children are e-safe is a vital part of our work and children are education about e-safety is spread in the following ways:

Pupils

- E-Safety is embedded as a key component of the Computing Curriculum. See the E-Safety Learning Roadmap from Rising Stars: switched On Computing for details.
- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- The eSafety policy will be introduced to the pupils at the start of each school year
- eSafety posters will be prominently displayed
- Rules for Internet access will be posted in prominent positions around school.
- Pupils will be informed that Internet use will be monitored.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.
- We will participate in Safer Internet Day every February.

Staff

- All staff will be given the School e-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 training in safe and responsible Internet use both professionally and personally will be provided.

Parents

- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and other similar ways
- Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school Web site.
- A partnership approach with parents will be encouraged. This will include parent / carers events with Internet safety demonstrations and suggestions for safe home Internet use.

Learning Platform – DB Primary

DB Primary features moderation, profanity filtering and a closed email system to keep pupils safe. There is also provide a whistle feature allowing children to instantly report anything that upsets them. All reports are sent to the teacher and E-Safety coordinator.

Internet Access

The Importance of the Internet in Learning in Schools
The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. Access to the Internet is a necessary tool for staff and pupils. It is an entitlement for children/pupils/pupils who show a responsible and mature approach. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in modern education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.
Pupils will use the Internet outside school and will need to learn how to evaluate the accuracy and quality of Internet information and to take care of their own safety and security.

Using the Internet to provide effective learning
Teachers, parents and pupils need to develop good practice in using the Internet as tool for teaching and learning. There is a fine balance between encouraging autonomous learning and maintaining adequate supervision. Systems that ensure Internet use is as safe as possible will enable increased use and the quality of that use is a critical factor. Internet access is provided by OneIT and includes a filtering system that is appropriate to the age of pupils (see 'Filters & Monitoring' section).

Internet access will be planned to enrich and extend learning activities.
The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.

- Pupils will be taught about acceptable Internet use.
- Pupils will be given clear objectives for Internet use.
- Access levels will be reviewed to reflect the curriculum requirement.
- Staff will select sites that will support the learning outcomes planned for pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be educated in taking responsibility for Internet access.

How pupils will be taught to assess Internet content
Pupils in school are unlikely to see inappropriate content in books due to selection by publishers and teachers. This level of control is not so straightforward with Internet-based materials. Therefore, teaching should be widened to incorporate Internet content issues, for instance the value and credibility of Web materials in relationship to other media. The tendency to use the Web when better information may be obtained from books will need to be challenged.

- Pupils will be taught ways to validate information before accepting that it is necessarily true.
- Pupils will be taught to acknowledge the source of information and observe copyright when using Internet material for their own use.
- Pupils will be made aware that the writer of an e-mail or the author of a Web page might not be the person claimed.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy. The evaluation of online materials is a part of teaching & learning in every subject.
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.
- Pupils will be taught to click on 'Hector Protector' if they feel uncomfortable with anything they access while online.

The availability of other Internet applications
The Internet is the underlying technology, but new applications are being developed to use this ability to communicate, such as blogs, Newsgroups and webcams. Many of these facilities have great potential for education, for instance pupils exchanging live text, speech or video with a similar class in another location around the country or world, at low cost. However, most new applications start without the needs of young users being considered, particularly the area of security.

- Pupils will not be allowed to access public chat rooms.
- Newsgroups or Blogs are password protected and only available to staff.
- New facilities will be thoroughly tested before pupils are given access.

The authorisation of Internet access

- Parental permission will be required before children can access the Internet and e-mail.
- Internet access is a necessary part of statutory curriculum. It is an entitlement for a pupil that is based upon responsible use.
- At Foundation Stage and Key Stage 1, the majority of the access to the Internet will be by teacher or adult demonstration. However, there may be situations when children have supervised access to specific approved on-line materials.
- At Key Stage 2, Internet access will be granted to a whole class as part of the scheme of work, after a suitable education in the responsible use of the Internet.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a permission form. This will be an indication by the parents and pupils that they have discussed, understand and accept the implications of the use the Internet in school and at home.

The assessment of risk when using the Internet in school
The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system. In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and work with OneIT to ensure reasonable precautions are in place to allow users access to appropriate material, including the use of filtering software. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a device.

E-mail

E-mail is an essential means of communication within education, and pupils use e-mail as part of our curriculum.

E-mail for Pupils:

- Pupils are provided an e-mail account through the learning platform DB Primary.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- E-mail must only be used in school for educational purposes.
- Pupils **will not** be allowed to access personal e-mail from the school system.
- Pupils may send e-mail as part of planned lessons. This assumes a high level of trust and pupils will be asked to sign the Acceptable Use Statement.
- In-coming e-mail will be regarded as public.
- Received e-mail may be examined.
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- A content filter is in place for all emails and flags are reviewed by the teacher and DB Primary administrator.

Email for staff:

- The school gives all staff & governors their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- Staff & governors should use their school email for all professional communication.
- 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 e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
- Delete all e-mails of short-term value
- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- Staff must inform (the eSafety co-ordinator Chris Story or line manager) if they receive an offensive e-mail
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Filters and monitoring

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Keeping Children Safe in Education (DfE, 2016)

The school uses Smoothwall to filter out in appropriate content. If children do see anything that upsets them, they can use 'Hector Protector' to cover the screen instantly so that the teacher can review the situation.

ICT authorised staff may monitor intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.,

All internet activity is logged by the school's internet provider. These logs may be monitored by that provider (One IT).

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Breeches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.
For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.
Policy breaches may also lead to criminal or civil proceedings.
The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

For pupils, reference will be made to the school's behaviour policy.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person (Chris Story). Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person (Chris Story).

E-Safety incidents are recorded on CPOMS, under the category 'E-Safety' and then relevant sub-category. This way, all child protection / safeguarding issues are kept in one place, allowing the relevant people to see 'the bigger picture'.

Social Media

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives. Our school uses Facebook and Twitter to communicate with parents and carers. Teachers are responsible for all postings on these technologies and monitors responses from others

- Staff *are not* permitted to access their personal social media accounts using school equipment during school hours
- The School will block / filter access to social networking sites and newsgroups for pupils unless a specific use is approved.
- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Social Media
- 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.
- Staff official blogs should be password protected and run from the school website with approval from the Senior Leadership Team. Staff must not run social network spaces for pupil use on a personal basis.
- Staff should not communicate with pupils or parents through their personal social networking applications and should ensure that their personal social networking applications are both secure and free from images and comments which may be regarded as unprofessional or bring the school or their profession into disrepute.

Children will be taught about the dangers of Facebook and that it is illegal for children under 13 to create an account. It is recognised that despite the law, and our insistence, some pupils may make social media accounts, and pupils in Y6 will be nearing the age in which it is legal. So that they are prepared, we teach children how to be safe online:

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils should be encouraged to invite known friends only and deny access to others.

The management of the school's web site

A well designed and regularly updated web-site can celebrate pupils work, promote the school and publish resources for projects or homework. Ground rules are important to ensure that the web-site reflects the school's ethos and that information is accurate and well presented. As the school's web-site can be accessed by anyone on the Internet, the security of staff and pupils must be considered carefully. Although common in newspaper reports, the publishing of pupils' names beside photographs that identify individuals is considered inappropriate on web pages. While any risks might be small, the parents' perception of risk has been taken into account in the devising of this policy.

- The Principal will delegate editorial responsibility to members of staff to ensure that content is accurate and quality of presentation is maintained.
- Pupils will be made aware that the quality of their work published on the Web needs to reflect the diversity of the audience.
- All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.
- The point of contact on the web site should be the school address and telephone number. Home information or individual e-mail identities will not be published.
- Full names will not be used anywhere on the Web site, particularly alongside photographs.

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used. Never interfere with any anti-virus software installed on school ICT equipment.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your OneIT, or Chris Story, immediately. OneIT will advise you what actions to take and be responsible for advising others that need to know.

Mobile Phones

Please see the 'Harrow Gate Primary Academy Mobile Phones Policy'.

Digital Images

Harrow Gate Primary School welcomes positive publicity. Children's photographs add colour, life and interest to school display and articles, promoting school activities and recognising and celebrating

success. We understand how this can increase pupil motivation and help the school and the wider community to identify and celebrate the school's achievements. However, in order to respect children, parent and staff rights to privacy and because of potential child protection issues, we recognise that all images must be used in a proper and responsible way, complying with the law and preserving the safety of children. Harrow Gate Primary Academy is committed to safeguarding and promoting the welfare of all children and expects all staff, pupils and their families to share in this commitment.
We seek to achieve a practical balance between the benefits of the use of digital image technology and compliance with data protection law and child protection issues as set out in the *"Data Protection Act 1998"* and *"Do We Have Safer Children in a Digital World? 2010".*

Data Protection Act 1998
Under the terms of the above act, images of pupils must not be displayed in any public place without the consent of parents/carers. Similarly, images of staff must not be displayed or published without their consent. All parents/carers are requested to sign an authorisation form.
Such publications may include:
Printed publications including internal and external publications e.g. school magazines, annual reports, newsletters and community magazines
School notice boards; i.e. display in public areas of the school
Media - including newspapers and TV
The school website where hosted photos will not be captioned with children's names; no personal details will be shared and group shots are preferred to individual shots

Child Protection
The school seeks parental permission for images of pupils to be used for any school, Enquire or any other publicity purposes. In all published images, pupils are to be appropriately dressed and positioned. There are to be no names and images published together unless prior specific consent is sought from parents. The Principal / Safeguarding Officer will also decide whether the publication of a photograph might pose a risk to any child who is considered "vulnerable". The The Principal / Safeguarding Officer will decide whether the publication of a photograph might pose a risk to a child.

Photographs and Video Filming by Parents/Carers
It is recognised that events such as school concerts, plays or sports days are activities which parents/carers will wish to record. Parents and carers are permitted to record or film digital images of their own children but are advised that such recordings are for their own "family album" and are not to be published in any form (social networks, internet web-sites).

Camera Phones/Staff Cameras/School Cameras
Pupils are not permitted to bring mobile phones into school and staff must not use personal phone cameras to record images of pupils. Similarly, staff are not permitted to use their own personal cameras in school to record pupil images. All teaching staff have access to iPods (the SLT have iPhones) with digital still and video cameras for this purpose as appropriate. Images should be stored centrally on the school network and content monitored by Principal / Safeguarding Officer and the E-Safety Leader

External Photographers
It is the school's responsibility to ensure that any photographer understands data protection considerations and is capable of meeting all responsibilities and obligations. The school must ensure that any external photographer has an up to date DBS check. The relationship between the school and the photographer can be regulated by a written contract which should include the following:
The photographer shall only use the visual images for the purposes indicated by the school;
Visual images shall be made available to the pupils or their parents only for personal use, either by the school itself or by the photographer.
Safe and secure storage arrangements.
The retention period.
The photographer will not have unsupervised access to children.

Retention Period

Any digital images taken, whether by the school or a commercial photographer, must be securely stored for a period not exceeding three years. Where visual images however form part of the historical records of the school these may be retained for an indefinite period of time.

Other Purposes
Information in relation to a child on admission in the school and for school record purposes (such as school reports) may include a visual image of the child. This does not require parental permission.

Complaints Procedure
Parents should follow the school's normal parental complaint procedure in most cases. Incidents of inappropriate or intrusive photography should be reported to the Head teacher / Safeguarding Officer or Governing Body. In the unlikely case of concerns regarding the use of photographs by the Press, complaints should be addressed to the "Press Complaints Commission" or the "Office of Communications" (OFCOM) in the case of TV companies.

Cyber Bullying

Children will be education about cyber-bullying as part of the E-Safety curriculum. Please see the 'Harrow Gate Primary Academy Peer-to-Peer Abuse Policy' for specific details.

Further sources of guidance relating to E-Safety

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

www.educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

APPENDICES

Appendix 1 -	Acceptable Internet use for all Staff.
Appendix 2 -	**E-Safety Rules for Internet Use Parent Copy**
Appendix 3 -	E-Safety Rules for Internet Use
Appendix 4 -	Child Internet, Video & Photography Consent
Appendix 5 -	Acceptable Use of ICT for Early Years, KS1 & KS 2Pupils

Appendix 1

Harrow Gate Primary Academy

ACCEPTABLE INTERNET USE STATEMENT FOR ALL SCHOOL STAFF

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school has an Internet Access Policy drawn up to protect all parties – the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

- Access should only be made via the authorised account and password that should not be made available to any other person.

- The security of the ICT system must not be compromised whether owned by the school, by Enquire Learning Trust, OneIT or any other organisation or individual.

- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed. Users should act on professional judgement and seek advice if unsure.

- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. School e-mail will not be used for personal use.

- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.

- Posting anonymous messages and forwarding chain letters is forbidden.

- Copyright of materials and intellectual property rights must be respected.

- All Internet use should be appropriate to staff professional activity or to pupil's education. However please note that:-

  - Use for personal financial gain, gambling, political purposes or advertising is forbidden.

  - Closed discussion groups can be useful but the use of public chat rooms is not allowed.

  - Users should follow any separate policies adopted from SBC relating to the use of Social Networking and any other websites.

  Members of staff are reminded that they should not deliberately seek out inappropriate/offensive materials on the Internet and that they are subject to the trusts recommended disciplinary procedures should they do so.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

Full name ..... Post .....

Signed ..... Date .....

Approved ..... Date .....

E-Safety and Responsible Internet Use
Parent Copy

Dear Parent / Carer,

The children are taught and reminded regularly about rules for keeping safe online. Please look at our E-Safety rules on the back of this letter. As part of pupils' curriculum enhancement and the development of ICT skills, we provide supervised access to the Internet in line with government expectations for all pupils in Key Stage 1 & 2. As part of the topics covered pupils in Years 3 to 6 may have access to an e-mail account.

Although there have been concerns about pupils having access to undesirable materials, we take positive steps to deal with the risks in school. Web filtering software restricts access to inappropriate materials. This is managed centrally by the local authority and is used in most schools in our local authority.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, we, or Stockton Borough Council cannot be held responsible for the nature or content of materials accessed through the internet. The council will not be liable under any circumstances for any damages arising from your child's use of Internet Facilities. Rules for the internet use are on the reverse of this letter.

The following information is taken from www.thinkuknow.co.uk (Educational web-site ran by Child Exploitation and Online Protection – CEOP) and is to help keep your child stay safe when accessing the internet.

- Know what your children are doing and who they are in contact with online.
- Ask them to teach you how to use any applications you haven't used before.
- Keep your computer in a family room so your child isn't alone while being online.
- Help your child understand that they should never give out personal details online, it is a public space so anyone could access what they have placed on the internet.
- Discuss what your child does online and remind them if they feel uncomfortable or unsafe to talk to you about it. It is never too late to tell someone if something makes them feel uncomfortable.
- Remember that the minimum legal age for a Facebook account is 13.

Please visit the web-site below for more information and useful resources.

www.ceop.gov.uk www.thinkuknow.co.uk www.getnetwise.org

Yours,

Harrow Gate Primary Staff.

Parent/Carer Permission

I give permission for my child to access the internet.

Signed:_____

Relationship to pupil:_____

Date:_____

Pupil's Agreement

I know what my teacher says about how to stay safe on the computer and I will follow the rules.

Signed:_____

Print Name:_____

Date:_____

Office Use Only

Updated on SIMS:_____ Date:_____

E-Safety Rules for Internet Use

We provide computers and Internet access as a research tool to help our learning.
The following rules will help keep everyone safe:

- I will use only my own username and password.
- To help protect other pupils and myself I will tell a teacher if I see anything I am unhappy with or if I receive a message I do not like.
- I will not access other people's files.
- I will use the computer only for school & homework.
- I will not bring memory sticks or DVD's into school without permission.
- I will ask permission from a member of staff before using the Internet.
- I will only e-mail people I know or those my teacher has approved.
- The messages I send will be sensible with no bad language.
- I will not give my home address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission.
- I will report any cyber bullying at home or school to an adult who can help stop it.
- I understand that the school can check my saved files and what websites I visit.

Internet, Video & Photography Consent
Parent Copy

Name of Child:……...

The Internet, Digital Video & Photography are key resources which can motivate and inspire children. This also forms part of our evidence to show how your child progresses through school. Whereas the risks are minimal, we have a duty of care towards pupils, which means they should remain unidentifiable and un contactable when using images of pupils on websites and videos.

In newsletters or other articles, we will only publish first names of children and **NEVER** surnames or addresses. Pictures used on our website will **NEVER** have children's names.

I **do / do not** consent to my child being photographed within school or on school visits.

I understand and agree that *(**PLEASE TICK** to indicate you have read and understood the statements):*

Photos and videos of my child may be used within school.

Photos and videos of my child may be used on the school website, on Twitter and for educational and newspaper publicity.

School nativities and assemblies may be filmed by family members of children in school. If I take photographs or videos on these occasions I understand that this is to be purely for the benefit of my family and I will **NEVER** post such photos or videos on social networking sites (e.g. Facebook, You tube) or other freely accessible media.

I have read and understand the **'E-Safety and Responsible Internet Use'** letter and give my consent for my child to access the Internet at school.

Name of Parent/Carer ……...

Signed……..Date……

Relationship to pupil ……

Office Use Only

Updated on SIMS:_____ Date:_____

Acceptable Use of ICT for Early Years Pupils

- I will take care when using the school ICT equipment and use it properly
- I will only share my password or login details with trusted adults
- I will tell an adult if I see anything which upsets me
- I will only take a photograph or video of someone if they say it is alright
- I will not deliberately write anything which upsets other people
- I understand that the school may talk to my parent or carer if they are worried about my use of school ICT equipment
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a period of time, even if it was done outside school

Acceptable Use of ICT for KS1 Pupil

- I will look after all the school ICT equipment and use it properly
- I will only share my password or login details with trusted adults
- I will tell an adult if I see anything which upsets me
- I will always ask before downloading from the internet or using material I have brought into school because I understand the risks from virus infections
- Any work I upload to the internet will be my own
- I will only take a photograph or video of someone if they say it is alright
- All of the messages I send will be polite
- I will not send messages which upset other people
- I will not give away my personal information or talk to people I do not know using the internet
- I understand that the school may check my use of ICT and talk to my parent or carer if they are worried about my eSafety
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a period of time, even if it was done outside school

Appendix 5

Acceptable Use of ICT for KS2 Pupils

- I will take care when using the school ICT equipment and use it responsibly
- I will keep my password and login details private unless required to share with a trusted adult
- I will inform an adult if I see or receive any unpleasant material or messages
- I will not interfere with anyone else's passwords, logins, settings or files on the computer
- I will be careful when downloading material from the internet or using material I have brought into school because I understand the risks from virus infections
- Any work I upload to the internet will be my own
- I know I need permission to take someone's photograph or to video them
- Any messages I post online or send in an email will be polite and responsible
- I will not send or forward messages or create material which is deliberately intended to cause upset to other people
- I know I must take care about giving away my personal information and making contact with people I do not know using the internet
- I understand that the school may check my use of ICT and contact my parent/carer if they are concerned about my eSafety
- I understand that if I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time and that this may apply even if the activity was done outside school.