Name of School: **Earls Barton Primary School**

Committee/ Person(s) Responsible**:** **Matt Passby**

Distribution : **Governors/ staff/ website**

Adopted date :

Review date:

Document Reviews

Version	Inclusion Governors	Adopted Full Govs	Comments	Initial
1.0				
1.1				

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.

Computing 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
- 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, such as tablets, with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

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, usually 13 years.

At Earls Barton Primary School, 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 other people 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 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 are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices (including laptops, webcams, whiteboards, voting systems, digital video equipment, Ipads etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband using the Talk Straight (schools broadband)
- National Education Network standards and specifications.

The school's Acceptable Use policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Security.

This policy has been adapted from an approved version developed by the Children and Young People's Service in consultation with Education Welfare - CYPS, Northamptonshire Police, the Local Safeguarding Children's Board Northamptonshire, Governors, Parents/Carers and Children, and in partnership with Professional Associates.

1. Writing and reviewing the Acceptable Use Policy

The Acceptable Use Policy should be read in relation to other policies including those for ICT, Behaviour, Anti Bullying, PSHE and Child Protection.

- Our Acceptable Use Policy has been written by the school, building on the NCC Draft Acceptable Use Policy and government guidance. It has been agreed by senior management and approved by the governors.
- The Acceptable Use Policy and its implementation will be reviewed annually.

2. Teaching and Learning

We teach our children how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively. The following skills will be taught during their time at the school:

- Beginning to make judgments about websites and emails received.
- An understanding of the risks from opening an email from a stranger.
- Beginning to use email as an effective form of communication between people they know.
- Some knowledge of search engines and how to use them accurately to find information.
- To navigate effectively around a webpage making judgements about the different areas and links.
- Beginning to make judgements about the use of personal information online.

We are following the new Computing curriculum linking it wherever possible into the topics being taught. Internet and email lessons in KS1 and KS2, are taught discreetly where each unit of work contains a lesson on online safety and we use the www.thinkuknow.co.uk resources, as well as a broadening bank of other available materials. These skills are also taught and modelled during an average school day as part of our broad and balanced curriculum, these skills and competencies are taught within the curriculum so that children and young people have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Children and young people will know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

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 students with quality Internet 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
- Children will have access to supervised email as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

2.3 Pupils will be taught how to evaluate Internet content and use it safely

- 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.
- Pupils will be taught never to give out personal details of any kind which may identify them or their location. i.e. full name, D.O.B, telephone number, e-mail address, school, clubs attended etc.
- Pupils will be taught online safety rules and shown how to turn off/close their monitor to safeguard them against anything which they are unsure about on the Internet.

2.4 PSHE

- The teaching and learning of online safety links with PSHE curriculum by ensuring that the key safety messages are the same whether children and young people are on or off-line engaging with other people.

3. Managing Internet Access and System Security

3.1 Information system security

- School ICT security will be regularly monitored.
- Virus protection will be updated regularly.
- School's Broadband (Talk Straight) will provide Internet access and a filtering service at a level suitable for primary school children.

3.2 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 that you use

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT technician.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and inform the ICT coordinator, Headteacher or IT technician immediately.

3.3 Data Security

- The accessing and appropriate use of school data is something that the school takes very seriously.

- The school is in adherence with GDPR. As such, if any work device (laptop/mobile phone/ipad or similar) is stolen it must be reported to the DPO immediately as this is considered a breach under GDPR and will need reporting within 72 hours.

- The school is aware of the Becta guidelines found at http://tinyurl.com/76gj9xr (published Spring 2009, please note that this organisation was closed in 2011 but the guidance is still useful).

- In conjunction with the advice and guidance given by the Information Commissioner's Office (ICO) http://www.ico.gov.uk/for_organisations/data_protection/security_measures.aspx

- And the Local Authority guidance documents MIS Data Management http://www.northamptonshire.gov.uk/en/councilservices/EducationandLearning/services/cypd_info/Pages/MIS-data-management.aspx

- The school gives relevant staff access to its Management Information System, with a unique username and password.

- It is the responsibility of everyone to keep passwords secure.

- Staff are aware of their responsibility when accessing school data.

- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.

- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data. Staff use encrypted laptops and memory sticks when working and storing sensitive data and documents.

- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight

- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.

- Staff have read, signed and agreed to adhere to the Staff Laptop Agreement which outlines how to keep portable hardware secure.

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when using shared copiers and wireless printers (multi-function printer, fax, scan and copiers).

- Anyone expecting a confidential or sensitive fax should notify the sender before it is sent.

3.4 Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is enabled with encryption.

- Store all removable media securely.

- Securely dispose of removable media that may hold personal data.

- All staff laptops are enabled with the encryption program Bitlocker to ensure all files containing personal, sensitive, confidential or classified data are encrypted.

- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

- Any equipment recycled is collected and disposed of using a company with a clear data protection policy, and transparent responsibility for checking and data has been

3.5 E-mail

- Pupils may only use approved e-mail accounts on the school system with adult supervision.
- Pupils may only send supervised e-mail to people known to them unless given specific permission.
- Pupils must immediately tell an adult 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.
- Staff, children and young people are to use their school issued e-mail addresses for any communication between home and school only. A breach of this will be considered a misuse and will result in independent access to use of an email account being withdrawn.
- Individual e-mail accounts can be traced if there is an incident of misuse whereas class e-mail accounts cannot.

3.6 Published content and the school web site

- The school address, e-mail and telephone number should be the only available contact details on the website.
- Staff or pupils' personal information will not be published.
- The School Administrator, alongside the Computing and Technology co-ordinator and Headteacher, will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.7 Publishing pupils' images and work

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or local press.
- Pupils' work will be published on the website in the form of displays. Individual names should not be linked with a specific piece of work.

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.

3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018.

3.10 Managing filtering

- The school will work with the LEA, DfE 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 online safety Coordinator.
- Senior staff will monitor the filtering methods closely, ensuring that they are appropriate, effective and reasonable.
- Pupils should use the search engine www.kidrex.org which uses Safesearch filters as a default setting. Other suggested sites with extra filtering levels: http://primaryschoolict.com/ www.safesearchkids.com/ http://www.squirrelnet.com.

.

4. Filtering and safeguarding measures

Staff, children and young people are required to use the Internet and all tools within it, in an acceptable way. Please refer to the Acceptable Use Rules for Staff and children and young people for the appropriate uses.

- **Schools Broadband (Talk Straight)** has a filtering system which is set at an age appropriate level so that inappropriate content is filtered with age appropriate tools.
- All computers, laptops, Ipads, notebooks and other devices are connected through the school network with an assigned computer name, IP address. Schools Broadband (Talk Straight) identify the IP addresses assigned to each machine and set a corresponding filtering level dependent on who has access to the machine. This is overseen and monitored by the IT technician in conjunction with the ICT co-ordinator and Headteacher.
- The levels listed below are in relation to age-appropriate categories. They give a standard blanket cover and can be altered and amended at any time through communication with Schools Broadband.

  - Level One **Pupil**: blocks access to- including but not exhaustive- gambling, dating, adult and sexual content, social networking, email (other than school assigned account), instant messaging and any other communication outside the school network.

  - Level Two **Staff**: blocks access to- including but not exhaustive- adult and sexual content, gambling, dating, social networking, phishing, any sites that pose a security risk.
  - Level Three **Admin**: open, excluding blocking potentially liable sites.

- Local Control – controls access to websites and provides the option to add to a 'restricted list' through contact with Schools Broadband.

- Anti-virus and anti-spyware software is used on all network and stand alone PCs, laptops and mobile devices, and is updated on a regular basis.

- A firewall setup and maintained by Schools Broadband (Talk Straight) ensures information about our children and young people and the school cannot be accessed by unauthorised users.

- Children are required to use a search engine with a child friendly filtering system.

- The wireless system is an on independent channel and encoded with a Network key to prevent hijacking.

- Staff should never leave an unattended machine logged in to the network.

5. Mobile phones and other technologies

- Mobile phones, Smart Phones and Personal Tablets are permitted on site for personal use only. No personal devices will be used for recording or communication involving children and young people under any circumstances.

- Staff members are not allowed to use their personal numbers to contact children and young people or parents, under any circumstances.

- Staff should not contact pupils or parents on any social networking sites under any circumstances.

- Other technologies schools and settings use with children and young people are:
  - *photocopiers*
  - *fax machines*
  - *telephone*
  - *cameras*
  - *Ipads*

6. Policy Decisions

6.1 Authorising Internet access

- All staff must read and sign the Acceptable Use Agreement 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 Foundation Stage, access to the Internet will be by adult demonstration or 1:1 supervision only. At Key Stage 1 and 2 access to the Internet will be by adult demonstration and include directly supervised access to specific, approved on-line materials and searches.
- Parents will be advised of the online safety rules in their child's first year of school and asked to sign and return an Internet Permission Form.

6.2 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 NCC 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.

6.3 Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

6.4 Community use of the Internet

- If appropriate the school will liaise with local organisations to establish a common approach to online safety.
- Wherever possible online safety speakers will be invited into the school to provide carers and parents with up to date information and guidance.

7. Communications Policy

7.1 Introducing the online safety policy to pupils

- Online safety rules will be posted near all networked notebooks and computers, and discussed with the pupils at the start of, and throughout each year.
- Pupils will be informed that network and Internet use will be monitored and will be made aware of the consequences of inappropriate use.

7.2 Staff and the online safety policy

- All staff will read the school Acceptable Use Policy and have its importance explained.
- All staff will have an opportunity to input into the content of the Acceptable Use Policy.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

7.3 Enlisting parents' support

- Parents' attention will be drawn to the School online safety Policy through a home school form and leaflet which they should read, sign and return. The policy is available on the school website and their attention will be drawn to online safety in terms of data protection and safeguarding in connection with performances, sports day and similar school events.
- Every effort is made to ask parents/carers to support our rules with their child or young person, which is shown by signing the Acceptable Use Rules together so that it is clear to the school or setting, the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school.
- Wherever possible training, discussion and updated information regarding online safety is offered to parents, including from outside agencies, and from within school.

8. Staff

8.1 Responsibility

It is the responsibility of all adults within the school setting to:

- Ensure that they know who the Designated Person for Child Protection is within school or other setting so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.
- Be familiar with the Behaviour, Bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed, immediately. In the event that a procedure is unknown, they will refer to the Headteacher immediately, who should then follow the Allegations Procedure, Section 12, LSCBN, where appropriate.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the online safety Leader.
- Alert the online safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of on-line technologies so that they know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- Be up-to-date with online safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the General Data Protection Regulation 2018.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- School bursars will need to ensure that they follow the correct procedures for any data required to be taken from the school premises.
- Report accidental access to inappropriate materials to the online safety Leader and Schools Broadband (Talk Straight) in order that inappropriate sites are added to the restricted list.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM and when transferring information from the Internet, on a regular basis, especially when not connected to the school network.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the NCC accident/incident reporting procedure in the same way as for other non-physical assaults.

8.2 Appropriate use by staff or adults

- Staff members have access to a filtered Internet service so that they can access age appropriate resources for their classes. They can create folders for saving and managing resources on classroom PC's, staff laptops and the laptops contained on the trolley.
- Staff members should not download or install software onto any school hardware without prior permission.
- Staff members should not capture, download or save any images of pupils on personal computers or devices.

- Staff members should not use social networking sites to communicate with any pupils or their parents.
- Staff members should not communicate personally with pupils using any personal devices, including mobile phones and email.
- Staff members know that they should not leave a computer or other device unattended whilst they are logged on to the Internet, email or staff files.
- All staff will receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed, returned to school to keep under file with a signed copy returned to the member of staff.
- When accessing school email, sites or data from home, the same Acceptable Use Rules will apply. Please refer to appendices for a complete list of Acceptable Rules for Staff.

8.3 In the event of inappropriate use

- If a member of staff is believed to misuse the Internet in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the Allegations Procedure (Section 12, LSCBN) and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.
  In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

9. Children

9.1 Responsibility

- Children are responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school or setting for the first time.
- Children are taught to use the Internet in a safe and responsible manner through computing, PSHE or other clubs and groups.
- Children are taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

9.2 Appropriate use by children and young people

- Acceptable Use Rules and the letter for children and young people and parents/carers are outlined in the Appendices and detail how children and young people are expected to use the Internet and other technologies within school or other settings, which includes downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the Internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

9.3 In the event of inappropriate use

Should a child or young person be found to misuse the on-line facilities whilst at school or in a setting the following consequences will occur (these will be reviewed by our stakeholders as the policy is updated):

- Any child found to be misusing the Internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules will result in not being allowed to access the Internet for a period of time and another letter will be sent home to parents/carers.
- A letter will be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

- In the event that a child or young person **accidentally** accesses inappropriate materials the child will report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing on-line technologies should also be addressed by the school.

- Children are taught about online safety as part of the Computing curriculum, and encouraged to consider the implications of misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

10. Links to other policies

10.1 Behaviour and Bullying Policies

- Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as e-mail. The school has an up to date Bullying Policy which will include any on-line bullying issues.
- All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all Computing and PSHE materials for children and young people and their parents/carers.
- Online behaviours should not be treated differently to offline behaviours and should have exactly the same expectations for appropriate behaviour. This is reflected within Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour of children, young people and adults.

10.2 Allegation Procedures and the Child Protection Policy

- Please refer to the Allegation Procedure, Section 12, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies which may result in an allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

- Allegations should be reported immediately to the Headteacher, or, Chair of Governors in the event of an allegation made about the Headteacher.
- The 2010 DFE White Paper clearly states that no personal equipment belonging to staff should be used when contacting children and young people about homework or any other school issues either in or beyond school and any such action should be dealt with.
- We follow this information to protect our staff members from potential allegations of misconduct by a child or parent.
- Please refer to the Child Protection Policy (Section 12 LSCBN) for the correct procedure in the event of a breach of child safety and inform the designated person for child protection within school immediately.

10.3 PSHE

We link the teaching and learning of online safety with our PSHE curriculum by ensuring that the key safety messages are the same whether children and young people are on or off line engaging with other people.

10.4 Health and Safety

Refer to the Health and Safety Policy and procedures of the school/setting and the County Council for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

10.5 School website

The uploading of images to the school website will be subject to the same acceptable rules as uploading to any personal on-line space. The uploading of any images is done in consultation with Parents signed agreement forms.

10.6 External websites

In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, or being discussed inappropriately on Social networking sites, the school are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

Further Information and Guidance

The nature of online safety is evolving. Encourage safe practice. You may want to keep up to date with further supporting documents, information or advice, which can be found on:

- www.ceop.police.uk (for parents/carers and adults)
- www.iwf.org.uk (for reporting of illegal images or content)
- www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)
- https://www.thinkuknow.co.uk/5_7/ (for 5 – 7 year olds)
- https://www.thinkuknow.co.uk/8_10/ (for 8 – 10 year olds)
- www.phonebrain.org.uk (for Yr 5 – 8)
- www.education.gov.uk (search for safety- for teachers/schools)
- http://www.northamptonshirescb.org.uk/ (Local Safeguarding Children's Board Northamptonshire – policies, procedures and practices, including Section 12 of the Allegations Procedures are available here)

Appendices

1. Pupil Internet Permission Form.
2 Online safety Leaflet.
3 Internet Rules Poster.
4 Acceptable Use Rules for staff.
5 Staff Procedures Following Misuse by Staff
6 Staff Procedures Following Misuse by Children and Young People

Appendix 1.

Internet Permission Form

Dear Parent/Guardian,

As part of a complete and enriched curriculum your child will be accessing the Internet and e-mail as an essential part of their learning.

In order to help protect your children from access to undesirable content, our school Internet Service provider operates a filtering system, in line with LEA requirements. This filtering system restricts access to inappropriate materials. Your child will be supervised at all times when they are using the Internet, and every reasonable precaution will be taken to protect your child from accessing undesirable material.

In order to support the school in educating your child about online safety, please read the following online safety Rules with your child then sign and return the form below. If you do not provide the necessary approval your child will have to be provided with limited access to ensure they can meet National Curriculum requirements. Please return the enclosed permission form, so that your child may use the Internet.

These rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and e-mail, both at school and outside of school (e.g. at a friend's house or at home).

I enclose a copy of the school Rules for Responsible Internet Use. Please contact the school for further information and to discuss any areas of concern.

Yours faithfully

Our Internet and E-mail Rules

- We use the Internet to help us learn.
- We only use the Internet when an adult is with us.
- We can send and open emails with an adult.
- We can write polite and friendly emails to people that we know.
- We know to ask an adult for help.
- If we see something we do not like we need to turn off or shut the screen and tell an adult.
- If we do not follow the rules we will no longer be able to use the Internet and email in school.

.....

Pupil Agreement:

Name:
_____Class:_____

- With an adult, I have read and understood the Rules for using the internet and e-mail safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Pupil Signature: _____Date:_____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision of pupils when using the internet and e-mail. I understand that on rare occasions inappropriate materials may be accessed and accept that school will endeavour to ensure this is infrequent and will deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the internet and e-mail facilities outside of school, that it is my responsibility to ensure safe and responsible use.

Parent/Carer Signature:_____ Date:_____

Appendix 4

Acceptable Use Rules for Staff

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or e-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Person for Child Protection or online safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Person for Child Protection is.

- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including social networking sites, my personal e-mail and should use the school e-mail and phones (if provided) and only to a child's school e-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or online safety Leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the General Data Protection Regulation 2018 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the online safety Leader.
- I have been given a copy of the Acceptable Use Policy to refer to about all online safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of online safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed…….Date…….
Name (printed)…….
School……...

Appendix 5

Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:
Report website to the online safety Leader if this is deemed necessary.
Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Ensure that no one else can access the material by shutting down.
Log the incident.
Report to the Headteacher and online safety Leader immediately.
Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
Inform the LA/RBC filtering services as with A.

C. An adult receives inappropriate material.
Do not forward this material to anyone else – doing so could be an illegal activity.
Alert the Headteacher immediately.
Ensure the device is removed and log the nature of the material.
Contact relevant authorities for further advice e.g. police.

D. An adult has used ICT equipment inappropriately:
Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately, if necessary.
Report to the Headteacher and Designated Person for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, LSCBN.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:
Preserve any evidence.
Inform the Headteacher immediately and follow Child Protection Policy as necessary.
Inform the RBC/LA/LSCBN and online safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Headteacher.

Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Child Protection Policy from the Local Safeguarding Children's Board Northamptonshire guidance.
All adults should know who the Designated Person for Child Protection is. It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Appendix 6

Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
Report website to the online safety Leader if this is deemed necessary.
Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list or use Local Control to alter within your setting.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed.
Reinforce the knowledge that it is illegal to access certain images and police can be informed.
Decide on appropriate sanction.
Notify the parent/carer.
Inform LA/RBC as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately.

Report to the Headteacher and Designated Person for Child Protection immediately.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or Innocent.
If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, LSCBN.
Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in school:
Preserve any evidence.
Inform the Headteacher immediately.
Inform the RBC/LA/LSCBN and online safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:
Preserve any evidence.
Inform the Headteacher immediately.

N.B. There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

- www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Child Protection Policy from the Local Safeguarding Children's Board Northamptonshire guidance.
All adults should know who the Designated Person for Child Protection is. It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.