Richard Durning's Endowed Primary

E Safety Policy

Updated: September 2023 *Renewal Date: September 2024*

Contents:

Policies and Documents in Support of this Document:

- *Remote Learning Policy*
- *Acceptable Use Policies*
- *Computing Curriculum Policy*
- *Acceptable User Agreements*
- *Permission Documents – use of pictures/video*
- *Mobile Phone Agreement*
- *Zoom Code of Conduct*
- *Keeping Children Safe in Education 2023*

Developing and Reviewing this Policy

This Online Safety Policy has been written as part of a consultation process involving the following people:

Emma Canavan, Rebecca Tilley, Catherine Hodgson, the teaching staff and Governors of Richard Durning's Endowed Primary School

It has been written using the most up to date guidance from the Department of Education document Keeping Children Safe in Education 2023 and any important updates added in September 2023.

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Created - Date: December 2020

Review Date – July 2023

The implementation of this policy will be monitored by Emma Canavan, Rebecca

Tilley and Catherine Hodgson

This policy will be reviewed as appropriate but at least every two years by the Computing Subject Leaders.

Lead Governor for Computing and e.safety is: Carl Culshaw

Online Safety Policy

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

ICT and the internet have become a vital resource in today's classroom and in the modern world. Knowing this, it is essential children are safeguarded when they are using the internet to ensure they do not have access to any inappropriate material. Pupils will be taught how to use technology, including social media, effectively and safely

Our E Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings.
This eSafety policy should be read in conjunction with the following other related policies and documents:

- Safeguarding / Child Protection
- ICT Acceptable Use Policy (for staff/governors, children & visitors (including supply teachers and students)
- Anti-Bullying
- Behaviour and Rewards
- Computing Curriculum Policy
- PSHE Policy
- Zoom Code of Conduct

2.Our school's vision for Online Safety

- Our school provides a diverse, balanced and relevant approach to the use of technology.

- The children are encouraged to maximise the benefits and opportunities that technology has to offer.
- The school ensures that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.
- Children are equipped with the skills and knowledge to use technology appropriately and responsibly.
- The school teaches everyone how to recognise the risks associate with technology and how to deal with them both within and outside the school environment (contextual safeguarding).
- All users in our school community understand why there is a need for an eSafety policy.

3. The role of the school's eSafety Champion

Our eSafety Champion is Emma Canavan.
The role of the eSafety Champion in our school includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's eSafety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an eSafety incident occur.
- Ensuring an eSafety Incident Log is appropriately maintained and regularly reviewed.
- Ensuring the Headteacher, SLT and subject leaders are responsible for checking filtering and monitoring systems within school.
- Keeping personally up-to-date with eSafety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging eSafety advice/training for staff, parents/carers and governors and ensuring all stake holders receive regular updates as required.
- Ensuring the Headteacher, SLT, staff, children and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

4. Security and Data Management

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment.

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data - Acceptable Use Policy (AUP).

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

- The Online Safety champion and Headteacher are responsible for managing information
- Staff know and are aware of their legal responsibilities
- Staff know that only approved means to access, store and dispose of confidential data are allowed
- Staff are only allowed to use removable devices in school if the documents contained on them contain no GDPR breach. Any documents with data on must be saved either on the school hard drive or on the cloud which is password protected.
- The school has backup systems in place to ensure the risk of data loss is addressed and managed.

5. Use of mobile devices (see appended Acceptable Use Policies (AUP's))

The use of mobile technology including cameras and sound recording devices offer substantial benefits to education but equally present schools with challenges particularly regarding publishing or sharing media on the Internet (e.g. on social network sites).

Mobile devices include:

- Laptops
- Tablets
- Mobile phones/smart phones
- Cameras
- Games consoles

Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of e-Safety. Many of

these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication.

Mobile devices can present a variety of challenges if not used appropriately and each school must define and document clear boundaries for their use. The Headteacher, SLT and subject leaders ensure there is appropriate filtering and monitoring is applied to devices using mobile and app content. They are valuable items that can be lost, stolen or damaged in the school environment and could also be considered as distracting or intrusive in a teaching or learning situation. However, staff and parents may equally have valid reasons why mobile phones should be readily available. Rules for the acceptable use of mobile devices have been discussed widely, communicated to all users including staff, visitors and parents.

- Use of mobile devices by children:
  - Children are not allowed mobile phones in school. If a child brings a mobile devise to school, it must be handed to a member of staff on arrival. It can be retrieved at the end of the school day.
  - Children are not allowed mobile devices on school trips.

Use of mobile devices by parents:

- We will not permit parents to use mobile technology on school premises and to record images/videos of their children at events (e.g. sports day / Christmas performance etc).
- All parents are asked to sign acknowledgment that this is the policy of the school (see Appendices – Photograph Consent)

- Use of mobile devices by visitors (supply teachers/students/contractors etc):

σ Mobile phones must not be used on the premises without direct consent of the Headteacher.

- Use of mobile devices by staff:

σ Mobile devices must be set on silent during working hours and kept out of site.
σ They must not be used during working hours or in front of children unless in an emergency.
σ Staff can check mobiles at break times.
σ Staff should inform family members that in an emergency they can be contacted via the school office.
σ During the infrequent times when the office is unmanned, a teacher or TA can check the office phone at regular intervals if they are expecting an urgent/emergency call.
σ Staff must not take photographs or videos of children in school on their mobile phone.

6. Use of CCTV, Video Conferencing, VOIP and Webcams

- Parents will be informed if CCTV, video conferencing or webcams are being used in the school.

- Parents have given permission for their children to participate in activities that include taking of video and photographs.
- School will seek parental permission for their child/children to participate in video conferencing activities. Although children may not appear 'live' on the Internet through a video conferencing link, it is important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast.

7. Communication Technologies

All digital communications must be professional in tone and content.

School uses a variety of communication technologies and needs to be aware of the benefits and associated risks. New technologies should be risk assessed against the potential benefits to learning and teaching before being employed throughout the school. Ideally this should be done before multiple devices are purchased. As new technologies are introduced, the eSafety Policy should be updated and all users made aware of the changes.

The following are examples of commonly used technologies in school:

7.1 Email:

In our school the following statements reflect our practice in the use of email:

- All staff have access to Microsoft 365 Office provided by Lancashire LEA.
- Staff should not, as a general rule, use personal email accounts during school hours and on school equipment. However, it is understood that there may be times when this is necessary. Staff should be mindful that emails could contain viruses which could compromise the school's ICT systems.
- The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts.
- Microsoft 365 Office has two factor authentication to ensure staff email accounts are secure and protected.
- All users are aware of the risks of accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- Subject leader to ensure all staff are regularly updated on cyber security. Staff, subject lead and lead governor take part in cyber security training.
- All users are made aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- Users are asked to report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

- All users are made aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act.

7.2 Social Networks:

Many adults and pupils regularly use Social Network sites, e.g.Club Penguin, Moshi Monsters, Facebook or Twitter, although the minimum age for registering for some of these excludes primary school pupils. These communication tools are, by default, 'blocked' through the internet filtering system (Netsweeper) for direct use in Lancashire schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute.
Personal use of social networking, and personal publishing sites, is included as part of staff induction, discussed regularly and outlined in the staff Acceptable Use Policy – along with sanctions for inappropriate use.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:
- If Social Network sites are used, staff and Governors must consider the purpose and audience and also ensure that the privacy settings and interactions are appropriate.
- Whatever methods of communication are used, individuals should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and potentially remains there forever.
- Be aware that the content on Social Network sites may be unmediated and inappropriate for certain audiences.
- If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- Staff are not permitted to communicate with parents, past pupils or siblings of pupils, especially if under the age of 18.
- Staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- For all staff and Governors, the content posted online should not:
o bring the school into disrepute o lead to valid parental complaints
o be deemed as derogatory towards the school and/or its employees
o be deemed as derogatory towards pupils and/or parents and carers
o bring into question their appropriateness to work with children and young people.

Adults must not communicate with pupils using any digital technology. Children must not be added as 'friends' on any Social Network site.

The school will take disciplinary action, in line with our Discipline Policy and Behaviour / Antibullying Policy, against a member of staff, Governor or pupil who posts inappropriate comments about the school, its staff, the children or parents, including acts of cyberbullying.

7.3 Instant Messaging & VOIP:

Instant Messaging systems, e.g. Text messaging, Skype, Facetime, are popular communication tools with both adults and children.

Our filtering system 'blocks' many of these services automatically.

Children and staff are taught about the risks involved in using such technologies (e.g. making unsuitable contacts, viewing inappropriate content etc).

The school uses a text messaging service to contact parents. This is only accessible by the Headteacher, Admin and School Staff. Personal information is stored securely by Teachers2Parents (further details available from www.teachers2parents.co.uk).

7.4 Virtual Learning Environment (VLE) / Learning Platform

School's chosen Online Learning Platform is Showbie, this will be used within the classroom environment, for homework and should home learning need to be provided.

See the Remote Learning Policy

7.5 Websites and other online publications

Information posted online is readily available for anyone to see and thus form an opinion about the school. From September 2012, the School Information (England) (Amendment) Regulations 2012 specified that certain up to date information must be made available on a school's website. More details regarding these requirements can be found on the DfE website or at
http://www.legislation.gov.uk/uksi/2012/1124/made

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

- A copy of the school's eSafety Policy is available on the school website.
- The children all sign an safety policy for children at the beginning of the academic year.
- Staff who administer the school website are aware of the guidance on the use of digital media online.
- No personal information will be published on the website other than names of staff and Governors (with their consent).
- The school website is only editable by the Headteacher, Admin Officer and Teaching Staff.
- The Headteacher is overall responsibility for what appears on the website.

- None of the school website's content is subject to copyright/personal intellectual property restrictions or is hidden behind a password protected area.
- Downloadable materials in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re-distributed without the school's consent.

8. Infrastructure and Technology, Filtering and Monitoring.

It is imperative that the school's infrastructure/network is as safe and secure as possible to meet the digital and technology standards in Keeping Children Safe in Education document.. Richard Durning's subscribes to the Lancashire Professional Development Service/BT Lancashire Broadband Service and internet content filtering is provided by default (Netsweeper). It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service.

Sophos Anti-Virus software is included in the school's subscription to Lancashire/BT Broadband Services. It is installed on all computers in school and configured to receive regular updates. Recently Updated 2023.

8.1 Children's access to Technology & Network

- Children are well-supervised when accessing school equipment and online materials.
- Children have their own folder on the network.
- Children's access is restricted to certain areas of the network (pupil network only)
- Any online learning platforms such as Purplemash, Showbie, reading eggs, mathletics all children have their own individual login and password.

8.2 Staff access to Technology & Network

- All staff aware of the guidelines in the Lancashire ICT Security Framework for Schools.
- All users of the school filter have a secure username and password.
- Staff reminded of the importance of keeping passwords secure.
- Passwords should be changed at least once a term for email.
- Access to school systems by staff are restricted according to their areas of responsibility (teacher network / admin&head network)

8.4 Software/hardware

- School has legal ownership of all software (including apps on tablet devices).
- Computing subject leaders keeps an up to date record of appropriate licenses for all software.
- Computing coordinator and computing technician regularly audits equipment and software (audit completed July 2020)
- Computing coordinator controls what software is installed on school systems.

8.5 Managing the network and technical support

- All servers, wireless systems and cabling securely located and physical access restricted where necessary.
- All wireless devices are security enable and are accessible only with a secure password.
- Relevant access settings have been restricted on tablet devices e.g. downloading of apps or 'inapp' purchases.
- Headteacher is responsible for managing the security of your school network. Governors review the safety and security of the school network annually.
- School systems are kept up to date automatically i.e. with critical software updates/patches.
- Users (staff & children) have clearly defined access rights to your school network.
- Staff and children are required to lock or log out of a school system when a computer/digital device is left unattended.
- Only admin users are allowed to download executable files and install software.
- Users report any suspicion or evidence of a breach of security to the Headteacher.
- School equipment should only be used in accordance with the 'Overview of Policy regarding Staff Laptops and Mobile Phones' (Appendix 1).
- All internal/external technical support providers are aware of our schools requirements / standards regarding eSafety.
- Headteacher and computing leads are responsible for liaising with/managing the technical support staff.

8.6 Filtering and monitoring

- Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, the Headteacher, Computing subject lead, lead governor should be doing all that they reasonably can to limit children's exposure to risks from the school's IT system. As part of this process, the Headteacher, Computing subject lead, lead governor governing bodies and proprietors should ensure school has appropriate filtering and monitoring systems in place and regularly review their effectiveness.

- All staff have an awareness and understanding of the provisions in place in regards filtering and monitoring and know how to escalate concerns when identified.
- The school uses Lancashire filtering services (Netsweeper).
- Filtering and monitoring is managed by the Headteacher, Computing support and Computing subject leaders and is reviewed at least annually.
- Members of staff are aware that devolved filtering is managed by the Headteacher, Computing support and Computing subject leaders.
- School laptops, including those used at home, are automatically updated with the most recent version of virus protection software used in school.
- Staff report suspected or actual computer virus infection to the Headteacher.
- Headteacher, SLT and Computing subject leader ensures the filters meet the digital and technology standards set out by the DfE in Keeping Children Safe in Education 2023.
- The filter (Netsweeper) blocks harmful and inappropriate content without unreasonably impacting teaching and learning.
- Lead governor reviews the standards and discuss with computing leads what more needs to be done to support school in meeting the schools safeguarding needs.

9. Dealing with Incidents

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 SIRO or eSafety Co-ordinator (C Hodgson/ E Canavan). 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 Headteacher.

eSafety Incident Log

Richard Durning's **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 or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere

* Can be found in the school office

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

Misuse and Infringements

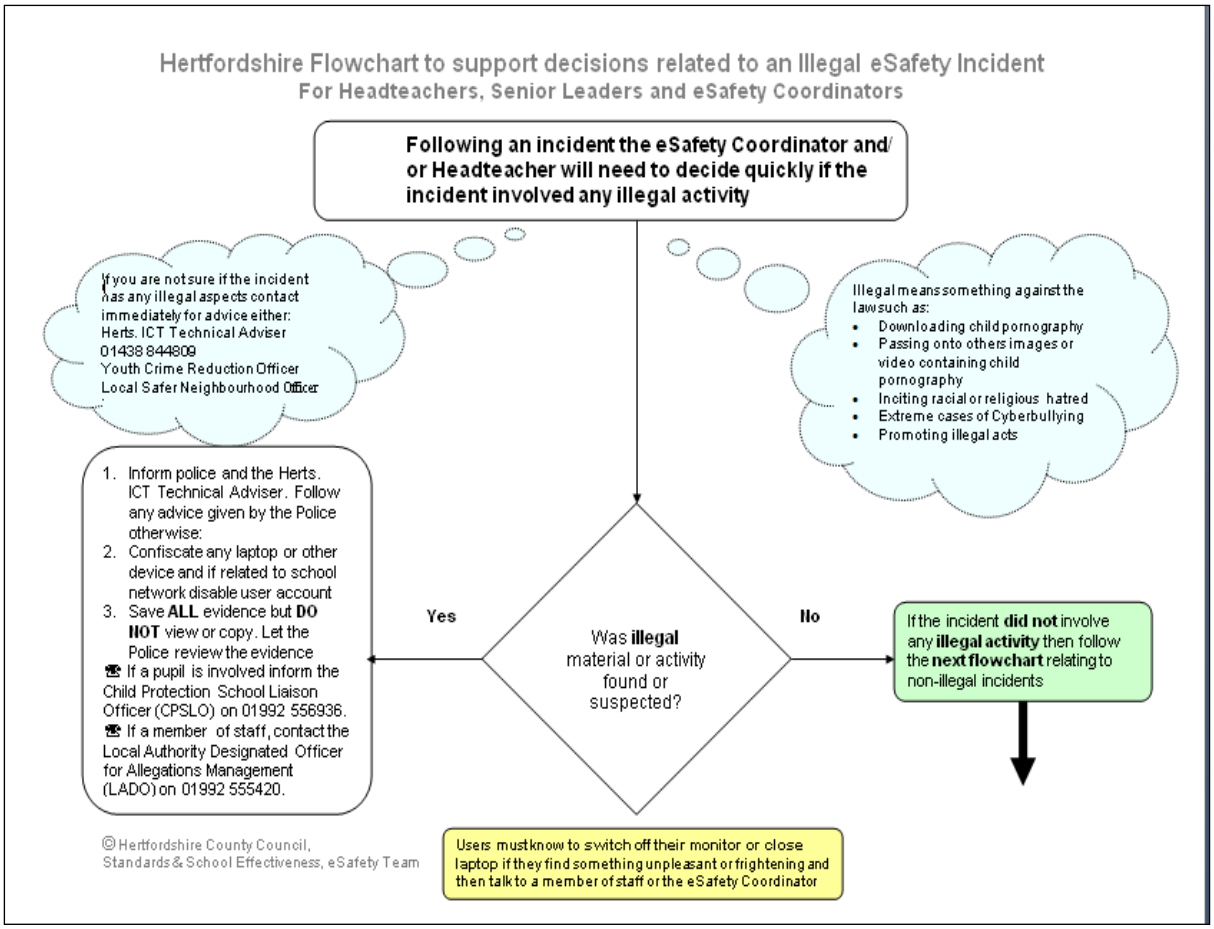
Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the flowchart below should be followed.

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; investigation by the Headteacher/ LA immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct

Flowcharts for Managing an eSafety Incident



9.2 Inappropriate use

It is more likely that our school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. The following may be considered when deciding what constitutes inappropriate use and the sanctions that may be applied.

Misdemeanour	Sanction/Action to be taken
Accidental access to inappropriate materials.	• Minimise the webpage/turn the monitor off/click the 'Hector Protector'/ 'CEOP' button. • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously. Deliberate searching for inappropriate materials. Bringing inappropriate electronic files from home. Using chats and forums in an inappropriate way.	• Inform Headteacher. • Additional awareness raising of eSafety issues and the AUP with individual child/class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement.

10. Acceptable Use Policy (AUP)

An Acceptable Use Policy is intended to ensure that all users of technology within school are responsible and are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

Richard Durnings has AUPs for Staff, Children and Visitors/Guests. These must be signed and adhered to by users before access to technology is allowed.

AUP's are regularly reviewed and updated.

See appendices.

11. Education and Training

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk (KCSIE 2023):

Area of Risk	Example of Risk
Content: Children need to be taught that not all content is appropriate or from a reliable source.	• Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse. • Lifestyle websites, for example proanorexia/self-harm/suicide sites. • Hate sites. • Content validation: how to check authenticity and accuracy of online content.
Contact: Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	• Grooming • Cyberbullying in all forms • Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords.
Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.	• Privacy issues, including disclosure of personal information, digital footprint and online reputation • Health and well-being - amount of time spent online (internet or gaming). • Sexting (sending and receiving of personally intimate images). • Copyright (little care or consideration for intellectual property and ownership – such as music and film).

Commerce: children need to be made aware that sometimes they can be tricked online to either buy goods gambling or trick websites that are used to get their money.

11.1 eSafety - Across the curriculum It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' eSafety.

School provides relevant, flexible and engaging eSafety education to all children as part of their curriculum entitlement and has considered the following points:

- Regular, planned eSafety teaching is provided within a range of curriculum areas - eSafety education is progressive throughout the school.
- eSafety education is differentiated for children with special educational needs. There is an additional focus on eSafety at pertinent points during the year (e.g. Safer Internet Day).
- Children are made aware of the impact of cyberbullying and how to seek help if they are affected by these issues, e.g. using peer mentoring or worry boxes.
- Children are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.

- Staff ensure that children develop an understanding of the importance of the Acceptable Use Policy and encourage them to adopt safe and responsible use of ICT both within and outside School.
- Children are reminded regularly of safe Internet use e.g. classroom displays, eSafety rules etc.

11.2 eSafety – Raising staff awareness

- eSafety training for all teaching and non-teaching staff ensures they are regularly updated on their responsibilities as outlined in our school policy.
- The ICT Coordinator will provide advice/guidance or training to individuals as and when required
- All staff are expected to promote and model responsible use of ICT and digital resources.
- At induction all new staff are directed to read the school's eSafety Policy and Acceptable Use Policy.
- eSafety Policy, Acceptable Use Policy, curriculum resources and general eSafety issues are discussed in staff/team meetings.

11.3 eSafety – Raising Parents Awareness

School offers regular opportunities for parents/carers to be informed about eSafety, including the benefits and risks of using various technologies both at home and at school, via the following means:

- School newsletters
- Website
- Workshops
- Other publications.

11.4 eSafety – Raising Governors' awareness A working party of Governors reviews the eSafety policy annually – this is then approved by the full Governing Body.

Governors are invited to attend eSafety workshops for parents/carers.

During the annual review of this policy, its impact will be evaluated and any relevant incidents reported to the Governors.