Market Weighton Infant School e-Safety Policy

2.1.1 Why is Internet use important?

The internet has become increasingly accessible for children in places like schools, libraries and their own homes. Children will experiment online, to enable them to take advantage of the many educational and social benefits of new technologies learners need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. However, all users (including our very young children) need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviours.

The Internet is a part of everyday life for education, business and social interaction. Market Weighton Infant School has a duty to provide children with Internet access. Internet use is part of the statutory curriculum and a necessary tool for learning. As our children get older, they begin to use the Internet more widely outside school and they therefore need to learn how to evaluate Internet information and to take care of their own safety and security at a simple level that they can understand.

The purpose of Internet use at Market Weighton Infant School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance Market Weighton Infant School's management functions.

2.1.2 How does Internet use benefit children?

A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet.
Benefits of using the Internet include:

- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- access to world-wide educational resources including museums and art galleries;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- access to learning wherever and whenever convenient.

2.1.3 How can we ensure Internet use enhances learning and life experiences?

Children need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

At Market Weighton Infant School, Internet access will be designed to enhance and extend education. Children will use the internet with support and be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Market Weighton Infant School will ensure that the copying and subsequent use of Internet derived materials by staff and children complies with copyright law.

Access levels will be reviewed to reflect the curriculum requirements and age of children. Staff should guide children to on-line activities that will support the learning outcomes planned for their age and maturity.

2.1.4 How will children learn how to evaluate content?

Information received via the Internet, email or text message requires good information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

The extent to which the internet is used by extremists as a tool for radicalisation is not fully known , but it is clear that that persons responsible for recent attacks have accessed and been influenced by the internet to varying degrees. Extremist websites may be used to disseminate propaganda, spread news and updates on extremist issues, add radical interpretation to theological tracts and provision of discussion forums for like minded individuals. The internet also offers easily accessible downloadable extremist material including advice and guidance on bomb making, filtered out of public systems, but often not at home – policies need to empower children and young people to evaluate content critically.

Children should be taught at a basic level how to be critically aware of the materials they read. The evaluation of on-line materials is a part of teaching/learning in every subject.

2.2.1 How will information systems security be maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and children. Data security is a complex matter and cannot be dealt with fully in this document. However, the person in charge of data security needs to be identified within the organisation; this could be a network manager, business manager, or technical manager. Note the role is distinct and separate from the 'E-safety co-ordinator', a role identified in 3.2.1.
All staff with access to personal data are liable in law to protect that data. Should data be lost from an unencrypted USB drive or seen on a laptop used by other people, the consequences could be serious for the member of staff, for the school or organisation.

Local Area Network (LAN) security issues include:

- Access to all ICT systems shall be via unique login and password. Any exceptions shall be recorded in the risk assessment and approved by the person in charge of data security.
- Where possible, all information storage shall be restricted to only necessary users. Access granted to new groups of users (for example, an external group attending a school-based event) shall be approved by the person in charge of data security.
- All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil personal storage) shall be authorised by the person in charge of data security. This shall include the authorisation of access required by the ICT Support Team during investigations.
- Where 'restricted' information is stored, access shall only be granted to individuals approved by the person in charge of data security. A record shall be kept of these approvals.
- All access controls should be reviewed each term, to ensure that any users that leave have their access removed.
- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes that compromise access or security and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be pro-actively managed and must be password protected.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils'/staff work areas or attached to email.
- Files held on the organisation's network will be regularly checked.
- The person in charge of network management will review system capacity regularly.

2.2.2 How will filtering be managed?

Levels of Internet access and supervision will vary according to the child's age and experience. Access profiles must be appropriate for all members of the organisation.

Market Weighton Infant School will use the LA mediated filtering systems to ensure that systems to protect children are reviewed and improved. Requests for filtering changes from within the organisation will be made via the Headteacher.

Organisations installing their own filtering systems are taking on a great deal of responsibility and demand on management time. Hundreds of inappropriate sites are created each day and many change URLs to confuse filtering systems.

Broadband access will include filtering appropriate to the age and maturity of children. A senior member of staff in the organisation will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the organisation believes is illegal must be reported to the appropriate agencies such as Children's Social Care, IWF or CEOP. See Response to Risk Flowchart.

2.2.3 How will videoconferencing be managed?

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in educational settings.
The National Educational Network (NEN) is a private broadband, IP network interconnecting the ten regional schools' networks across England with the Welsh, Scottish and the Northern Ireland networks.

Schools with full broadband are connected through the YHGfL and have access to services such as gatekeepers and gateways to enable schools to communicate with external locations.
Conferences should always be booked as private and not made public. The conference URL should only be given to those who you wish to take part.

Possible Statements
The equipment and network
- All videoconferencing equipment must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- Videoconferencing equipment should not be taken off Market Weighton Infant School premises without permission.

Users
- Videoconferencing should be supervised appropriately for the young person's age.
- Parents and carers should agree for their children to take part in videoconferences, probably in the annual return.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the videoconferencing services should only be issued to members of staff and kept secure.

Content
- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.

2.2.4 How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom and/or organisational use. The safest approach is to deny access until a risk assessment has been completed and safety established.

Virtual online classrooms and communities widen the geographical boundaries of learning. The safety and effectiveness of virtual communities depends on users being trusted and identifiable.

There are dangers for employees/volunteers however if personal phones are used to contact children and therefore an organisationally owned phone should be issued if required.

The sending of abusive or inappropriate text, picture or video messages is forbidden. Abusive messages should be dealt with under the behaviour and anti-bullying policies.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the organisation is allowed.

The school allows staff to bring in mobile phones and devices, but these must be switched off or be on silent during working hours.

Staff and volunteers are requested not to use their own IT equipment (such as cameras) in school without prior permission of the headteacher. This includes the use of personal cameras and mobile phones to take images of children or show images to children.

The school does not allow children to bring in mobile phones.

2.3.1 How should personal data be protected?

The quantity and variety of data held on children, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

The eight principles are that personal data must be:
- Processed fairly and lawfully;
- Processed for specified purposes;
- Adequate, relevant and not excessive;
- Accurate and up-to-date;
- Held no longer than is necessary;
- Processed in line with individual’s rights;
- Kept secure;
- Transferred only to other countries with suitable security measures.

Organisations will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

2.3.2 Password security

Members of staff/volunteers with access to ICT systems shall be responsible for taking the appropriate steps to select and secure their passwords. These steps should include:

- Keeping their password secure from others.
- Using a different password for accessing organisational systems to that used for personal (non-organisational) purposes.
- Choosing a password that is difficult to guess, or difficult for others to obtain by watching them login.
- Adding numbers or special characters (e.g. !@£$%^) can help.
- Changing passwords regularly e.g. every three months.
- Staff/volunteers should try not to write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else.
- In addition, when leaving a computer for any length of time, all staff members/volunteers shall log off or lock the computer, using CTRL+ATL+DELETE or other system command.

2.3.3 How will email be managed?

The implications of email use for Market Weighton Infant School by children need to be thought through and appropriate safety measures put in place. Un-regulated email can provide routes to children that bypass the traditional Market Weighton Infant School boundaries.

Children will only email each other or staff through the Learning Platform. Children must immediately tell an adult if they receive offensive email. Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

The school email address will be used for communication outside of the school.

2.3.4 How will published content be managed?

Excellent websites can inspire children to publish work of a high standard. Websites can celebrate children's work, promote Market Weighton Infant School and publish resources for projects.

Sensitive information about Market Weighton Infant School and children could be found in a newsletter but Market Weighton Infant School's website is more widely available. Publication of information should be considered from a personal and Market Weighton Infant School security viewpoint. Material such as employee/volunteer lists or a plan may be better published in a handbook or on a secure part of the website which requires authentication. To this end:

- Named photographs of staff will not be published on the school website.
- The contact details on the website should be the Market Weighton Infant School address, email and telephone number. Employee/volunteer or children's personal information must not be published.
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. consider replacing ‘@’ with ‘AT’).
- The appointed senior leader will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with Market Weighton Infant School guidelines for publications including respect for intellectual property rights and copyright.

2.3.5 Can pupil images and work be published?

Strategies include using relatively small images of groups of children and possibly even using images that do not show faces at all. “Over the shoulder” can replace “passport-style” photographs but still convey the organisational activity. Personal photographs can be replaced with self-portraits or images of children’s work or of a team activity. Children in photographs should, of course, be appropriately clothed.

Images of children should not be published without the parent’s or carer’s written permission. Written permission from parents or carers will be obtained before images of children and young people are electronically published. These images can then be published on our own Learning Platform which is accessed by Market Weighton Infant School parents. However, if a child's face is clearly identifiable, permission will still be sought before publication on the school website. Children’s full names will not be used anywhere on the website, particularly in association with photographs.

Children also need to be taught the reasons for caution in publishing personal information and images online.

2.3.6 How will social networking and personal publishing be managed?

Parents/carers and professionals need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.

Children should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All adults should be made aware of the potential risks of using social networking sites or personal publishing either professionally with children or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. The internet and social networking sites may provide a virtual online community to which a young person may wish to belong and then may in turn become increasingly exposed to extremism. Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger and many others. Market Weighton Infant School will control access to social media and social networking sites.

Children will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc. Children should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the child or young person or his/her location.

Photographs taken by parents at school events may not be allowed if parental permission of all children involved is not gained or if there are any ongoing child protection issues known by the school. This will be at the discretion of the headteacher and made clear to parents at the start of an event. Parents should be advised not to publish photos of children on the Internet or social networking sites without the permission of the parents or carers of all the children in the image. This should be for personal use only in accordance with the Data Protection Act 1988.

Employee/volunteer should be advised not to run social network spaces for children and young people’s use on a personal basis.

Children should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children should be encouraged to invite known friends only and deny access to others by making profiles private.

Children are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

2.4.1 How will Internet access be authorised?

All staff/volunteers and children are granted access to the Internet and there is a list of staff and children who have access to email. All staff/volunteers must read and sign the organisation’s policies regarding information security and the use of information technology before using the organisation’s ICT resource.

Pupil usage should be fully supervised by an adult and in line with the Acceptable Use Policy (AUP).

Parental permission shall be required for Internet access in all cases — a task that is organised when children join the school. Parents/carers are asked to sign and return a consent form for children's access in accordance with the Acceptable Use Policy (AUP). Parents/carers will be informed that children and young people will be provided with supervised Internet access, but must comply with the AUP at all times.

2.4.2 How will risks be assessed?

E-security and e-safety is based upon the assessment of risk, and the implementation of controls to manage these risks; no use of digital technology is completely risk free. Information security is critical, in both protecting the information held concerning staff/volunteers, children and young people, and in ensuring the reliability of ICT systems to support teaching and learning.

As a minimum, the risk assessment shall be updated and reviewed annually by the Senior Leadership Team and reported to the Governing Body. It is recommended that a review should be conducted each term.
As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The organisation will need to address the issue that it is not possible to completely remove the risk that children might access unsuitable materials via the system. To this end, Market Weighton Infant School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer. Neither Market Weighton Infant School nor ERYC can accept liability for the material accessed, or any consequences resulting from Internet use.

Market Weighton Infant School should audit digital technological use to establish if the e–safety policy is adequate and that the implementation of the e–safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

2.4.3 How will complaints be handled?

Parents and staff should know how to use the organisation’s complaints procedure.

Potential child protection and illegal issues must be referred to the Designated Child Protection Co-ordinator and/or E–safety Co-ordinator. Please refer to the Response to Risk Flowchart for reporting e-safety incidents.

Complaints of Internet misuse will be dealt with under Market Weighton Infant School's Complaints Procedure. Any complaint about staff misuse must be referred to the E-safety Co-ordinator. All e–safety complaints and incidents will be recorded by Market Weighton Infant School — including any actions taken. Parents/carers will be informed of the complaints procedure. Parents/carers will work in partnership with Market Weighton Infant School to resolve issues. Any issues (including sanctions) will be dealt with according to Market Weighton Infant School disciplinary and child protection procedures.

2.4.4 How should the Internet be used across the community?

Internet access is available in many situations in the local community. Organisations are developing access appropriate to their own client groups and children may find variations in the rules and even unrestricted Internet access. Although policies and practice may differ, community partners adhere to the same laws as schools. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with children and young people on the reasons for the differences could be worthwhile.

Sensitive handling of cultural aspects is important. For instance, filtering software should work across community languages and school Internet policies may need to reflect the children and young people’s cultural backgrounds. Assistance from the community in drawing up the policy could be helpful.

The school may liaise with local organisations to establish a common approach to e–safety. The school will be sensitive to Internet related issues experienced by children and young people out of school, e.g., social networking sites, and offer appropriate advice.

2.4.5 How will Cyberbullying be managed?

Cyberbullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” (DCSF 2007).
It is essential that children, organisations, and parents/carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyberbullying (along with all forms of bullying) will not be tolerated in Market Weighton Infant School. There will be clear procedures in place to support anyone affected by cyberbullying. All incidents of cyberbullying reported to Market Weighton Infant School will be recorded.

There will be clear procedures in place to investigate incidents or allegations of cyberbullying:

- Children, staff/volunteers and parents/carers will be advised to keep a record of the bullying as evidence.
- Market Weighton Infant School will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended for the user for a period of time.
- Parents/carers will be informed.
- The Police will be contacted if a criminal offence is suspected.

2.4.6 How will Learning Platforms and VLEs be managed?

The Learning Platform/Environment (LP) must be used subject to careful monitoring by Senior Leadership Team/Senior Manager. As the usage grows, then more issues could arise regarding content, inappropriate use and behaviour online by users. The Senior Leadership Team/Senior Manager has a duty to review and update the policy regarding the use of the Learning Platform annually and all users must be informed of any changes made.

Senior Leadership Team/Senior Manager and staff/volunteers will monitor the usage of the LP by children and staff regularly in all areas, in particular message and communication tools and publishing facilities. Children/staff/volunteers will be advised on acceptable conduct and use when using the learning platform. Only members of the current pupil, parent/carers and staff community will have access to the LP. All users will be mindful of copyright issues and will only upload appropriate content onto the LP. When staff, children and young people etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the LP for the user may be suspended.
d) The user will need to discuss the issues with a member of Senior Leadership Team/Senior Manager before reinstatement.
e) A pupil's parent/carer will be informed.

2.4.7 Response to an Incident of Concern

An important element of e-safeguarding is the ability to identify and deal with incidents of concern and related to the confidentiality of information. All staff/volunteers and children have a responsibility to report e-safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The organisation shall establish an incident reporting procedure and record reported incidents in an Incident Log (see attachment).

The Incident Log shall be formally reviewed, and any outstanding actions delegated, by the Senior Leadership Team/Senior Manager within the organisation at a minimum frequency of once per term. Through this review process, where deemed appropriate, management shall update the risk assessment in light of new incidents. The Log and accompanying action plans should be reviewed annually by the Governing Body.

Organisations could usefully draw up a list of common incidents from the log. For example:

Possible statements:

- Circumventing the network security system
- Accessing inappropriate material (definition should be in AUP)
- Installing unapproved software
- Using other people's accounts, email addresses or passwords
- Breaching copyright
- Uploading school material onto a social network or chat room
- Leaving school mobile devices unattended
- Not logging off when leaving a device

Child Exploitation and Online Protection (CEOP)

Adults and children need to know how to block someone online and report them if they feel uncomfortable. It is important to realise that there are people other than the staff in your organisation who can help. Online child abuse can be reported directly, as well as requests to seek out more advice and support. Reports can be made directly to CEOP through their Click CEOP reporting button, which is present on an increasing number of websites and social networks.

2.5.1 What should the communications plan contain?

Market Weighton Infant School shall include appropriate communications and/or training for all sectors of the organisation's community.

This should cover:

- Workforce training in understanding the rationale for all e-safeguarding procedures and the consequences of inappropriate practice.
- Workforce training in responsible approaches to data on mobile devices, communicating online and procedures when using multimedia digital content such as photographs, videos and podcasts in terms of permission seeking, taking, storage and retention.
- A comprehensive and developmental e-safety curriculum for children referenced to planning.
- The programme should include the responsible use of web and communication technologies both inside and outside school and risks related to cyberbullying.
- Regularly re-visiting of the AUP with staff and pupils.
- ICT non-teaching staff training related to how digital technology can enhance learning and teaching.
- Organisations shall create working Acceptable Use Policies (AUPs) based on all the agreed procedures for e-security and e-safety and covering ICT usage by all sectors of the organisational community. This policy shall be subject to annual review by the governing body.

Organisations like ChildNet, ThinkyouKnow, CEOP offer support for education and training materials.

2.5.2 How will the policy be introduced to children and young people?

The children and parent agreement should be attached to a copy of the organisation's e–safety AUPs appropriate to the age of the pupil.

Consideration must be given as to the curriculum place for teaching e–safety; it could be as an ICT lesson activity, part of the pastoral programme or part of every subject whenever children are using the internet.

A useful checklist could include:-

- Every child to be informed that network and Internet use will be monitored.
- Children's instruction in responsible and safe use should precede Internet access and be age appropriate.
- Safe and responsible use of the internet and technology is reinforced across the curriculum.
- Particular attention to be given where children are considered to be vulnerable.
- Opportunities for confidential discussions and pastoral support to supplement the planned curriculum.

Useful e–safety curriculum resources and programmes include:

- ThinkUKnow: www.thinkuknow.co.uk
- Childnet: www.childnet.com

2.5.3 How will the policy be discussed with staff?

It is important that all staff/volunteers feel confident to use new technologies in teaching and the organisation's e–safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

Particular consideration must be given when staff are provided with devices by the organisation which may be accessed outside of the organisational network. Organisations must be clear about the safe and appropriate use of organisational provided equipment and rules about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of the organisation's information.

All staff within Market Weighton Infant School including administration, governors and volunteers shall be included in awareness raising and training. Induction of new staff/volunteers shall include a discussion of the organisation's e–safety Policy.

The e–safety Policy will be formally provided to and discussed with all members of staff.To protect all staff and children, the organisation will implement Acceptable Use Policies.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Manger/ Team and have clear procedures for reporting issues.

Staff training in safe and responsible Internet use both professionally and personally will be provided.

2.5.4 How will parents' support be enlisted?

Internet use in children's homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents/carers are aware of the dangers, children may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents/carers plan appropriate supervised use of the Internet at home and educate them on the risks. Parents/carers should also be advised to check if their child's use elsewhere in the community is covered by an appropriate use policy. One strategy is to help parents/carers to understand more about ICT — perhaps by running courses and parent awareness sessions.

Parents'/carers' attention will be drawn to Market Weighton Infant School's e-safety Policy in newsletters, the prospectus and on the Market Weighton Infant School website as well as through the organisation's Child Protection Policy and Procedures. A partnership approach with parents/carers will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–safety at other attended events e.g. sports days. Parents/carers will be requested to sign an e–safety/Internet agreement as part of the Home School Agreement. Information and guidance for parents/carers on e–safety will be made available to parents/carers in a variety of formats.

E-Safety Co-ordinator- S. Kay-Wood
E-Safety Governor- H. Beales