THE MEADOWS PRIMARY SCHOOL
E-SAFETY POLICY

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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. The e-Safety policy relates to other policies including those for ICT, bullying and for child protection.

Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior leaders and approved by governors.
It is designed to clarify issues pertaining to filtering and Internet monitoring for the all users of the school network, whether adults or children.
It has been updated in line with recent GDPR legislation.

Filtering

- The Meadows Primary School maintains a single point of access to the Internet through a central connection to the county internet service - E2BN. At this access point, F1 provide the school with an internet filtering system, which blocks material inappropriate to children.
- Among the items filtered are obscene visual images, strong language, pornography, blogs/chat sites and social media sites including Twitter, Facebook, Instagram and YouTube.
- The staff filter allows access to reviewed sites that may provide useful educational resources/video clips for use in classrooms.
- It should be noted that, due to the nature of the internet, no filtering system can be perfect; therefore, the service provided to The Meadows Primary School has the ability to add additional blocked sites or to remove sites found to be inappropriately blocked.
- If staff or pupils come across unsuitable online materials, the site must be reported to the e-safety leader.

Monitoring

- The teacher or staff member supervising any pupil has the primary responsibility of monitoring the internet for pupil safety and appropriate use.
- Pupils are prohibited from using the internet without the direct supervision of a teacher or staff member. The service provides a monitoring system that can record the internet sites accessed.
- Pupils will be taught how to use the internet wisely, and to refer to the school guidelines when making choices. All classes display safe internet use rules at an age-appropriate level.

Messaging and Social Networking

- Messaging includes posting items such as text to a bulletin board, discussion groups, use of email, and chat features including instant messaging. Pupils are prohibited from using messaging.

- Social networking sites such as Facebook, Twitter, YouTube and Instagram are permanently blocked on the school system for pupils. Pupils cannot log onto, or search these sites within school.
- Parents have the opportunity to sign up to text alerts and to receive letters by email. Parents' contact details are held in strict accordance with general data protection regulations (GDPR). Communication via text and email is undertaken by members of the school admin team or SLT, and messages are checked by a third party before being sent.

Responsibility

- Each user must take responsibility for his or her use of the computer network and internet. Children and adults within school are expected to abide by rules for safe and appropriate use of the system.
- If a pupil accesses an offensive or harmful site by mistake, they must click on the home button or switch off the monitor and report what has happened to a member of staff. Similarly, if a pupil notices that another pupil has accessed such a site, they must also report it to a member of staff.
- These responsibilities are clearly laid out for pupils in the school's internet safety guide, which is shared with all pupils and displayed both in the ICT suite and within classrooms (link to the 'monitoring' section).

Identification of Pupils on the Web

- Pupils' work published on the web will not be identified by surname.
- Including photographs of groups of pupils on the school website can be motivating for the pupils involved, and provide a good opportunity to promote the work of the school; such photographs will only be used for educational purposes and the identity of children will be protected.
- The full name of a pupil will never be included alongside the photograph.
- Children's names will not appear on school tweets, nor close-up pictures of faces. Parents and carers will complete consent forms, upon joining the school, if they do not wish their child to appear on social media and/or on the school website and/or school publicity materials. Photographs of pupils will only be used if parental permission has been granted. Permissions were updated under new general data protection regulations (GDPR) in 2018.

Use of mobile phones

- The use of mobile phones by children in school is not permitted. On occasions, parents may request permission for a child to bring a mobile phone into school. In these cases, children's phones must be deposited securely at the school office at the start of the school day, and then collected at the end of the day.
- Staff may use mobile phones within the staff room. Mobile phones should not be used at times when children are present in school, and should not be used within classrooms. Staff should never use their mobile phones as a means of taking photographs within lessons (see paragraph below).

- The use of mobile phones is prohibited by all visiting adults, including parents, carers and contractors, while on the entire school premises, including within the school building.

Use of iPads

- Class iPads will be used to collect photographs of the learning environment for the purpose of teacher assessment. These may be transferred to the school's secure G:Drive for storage purposes. Staff should never share any of the photos taken in school with third parties, or transfer them in other locations beyond the school environment. After being uploaded to the secure school storage drive, the photographs must be deleted.

E-Safety Education

- Pupils will be taught about safe use of the internet within school sessions at an age-appropriate level. The National Curriculum is followed.
- A guide to 'SMART' use and rules/expectations will be displayed in each learning area where computers and iPads are regularly used.

All adults within school will undertake training in e-safety annually. It will focus on an understanding of **online risk, which can be addressed within the following categories:**

- Grooming
- Online Bullying/Trolling
- Harmful Content
- Digital Footprint (Long term implications of online sharing)

Parents and carers attention will be drawn to the school e-safety policy in newsletters, the school brochure and on the school website.

Security

- The Meadows Primary School provides a secure network for the school community through the county network - E2BN
- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any ICT school resource.
- Any person not directly employed by the school will be asked to sign an 'acceptable use' agreement before being allowed to access the internet from the school site.
- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Lincolnshire County Council can accept liability for any material accessed, or any consequences of internet access.
- All staff will be given the school e-safety policy and its importance explained.
- F1 Group will manage filtering systems and this in turn will be supervised by the SLT. A communications book, located in the staff room, will be used to report issues which need to be addressed.

- Staff will always use a child-friendly safe search engine when accessing the web with pupils.

Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by a member of the SLT.
- Any complaint about staff misuse must be referred to the headteacher.
- Any complaint of pupils' misuse, either at home or at school must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Confidentiality of Pupil Information

- Personal information concerning The Meadows Primary School pupils will not be disclosed or used in any way on the school website, social media or school publicity materials without the specific permission of a parent or guardian. Pupils are not permitted to provide private or confidential information about themselves or others on the internet.

Remote Learning

In the event of school closures or the need for families to self-isolate for a period of time, Seesaw online learning platform is used to allow children access to teaching and learning materials at home. Seesaw is an online platform used for sharing teaching inputs on video and setting learning tasks. Parents are asked to log in to the secure system using a unique class code. Children can upload photos of their work, respond to tasks onscreen and read comments from staff about their learning.

- All 'classes' created within Seesaw are administrated by SLT and work/comments are reviewed on a daily basis
- No comments or uploads by children or families can be viewed anyone other than the assigned teachers registered to the class.
- All comments/uploads must be reviewed by the assigned teacher, or one of the school Seesaw administrators (AB/TH) before they can be 'approved.' If they do not comply with safe working expectations, they will be deleted and the child/family contacted to discuss what action will be taken. The school reserves to delete an account if it is felt to be necessary.
- All children have reviewed rules and expectations for using Seesaw, and the usual school code of conduct will apply if the platform is used inappropriately or unsafely.

APPENDIX

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. With this in mind, parents and carers will be invited to attend training sessions in safe internet use on an annual basis. The following guidelines will be used when discussing use of the internet with children:

Recommendations for Internet use by pupils at home
Personal Safety for Children

When using the Internet:

- Children should never reveal personal information such as their name, home address or phone number or any information that might allow someone to locate them.
- Children should never agree to meet a person face-to-face whom they have “met” on the Internet without their parent’s permission and without an adult being present.
- If someone attempts to arrange a meeting with a child through the Internet, the child must report this communication to their parent or guardian.
- Instant messaging should not be used by children at home unless explicitly approved and supervised by parents.
- Children should choose screen names carefully, and not reveal their identities.
- Children should never phone an online ‘acquaintance’ without parental permission, because caller ID can trace a phone number and from that information, the child's address can be found.
- Nobody should reply to harassing, threatening or sexual messages but should report any such communication immediately to the police.

Filtering at home

- There are a number of filtering programs that allow parents to block sites and monitor their child’s use of the Internet, including the time of day, number of hours and types of access (such as chat, web, or newsgroup activities). It is recommended that parents use this type of filtering if their child will be using the internet without direct parental supervision. Filtering can be set to restrict all internet use when parents are not home.
- For more information, refer to:

http://www.childnet-int.org/
http://www.getnetwise.org/
http://www.safekids.com/

Location of Computers in the Home

- It is recommended that parents place computers used by children in a heavy traffic area of the home. The best place for a home computer used by a child is in an area such as the living room or kitchen.

Parent / Child Dialogue

It is recommended that parents:

- Have constant dialogue with their child about what they are doing online
- Encourage their child to show them what they are doing
- Consider establishing a "Code for Internet Use" for the home.

Violations

- The internet has much value in today's world and is available in many public places, including our smartphones. If a child violates the home "Code of Internet Use", it is recommended that parents try to use the situation as an occasion for learning in the first instance, rather than immediately "pulling the plug" on all home internet access.
- The school website contains links to several helpful organisations which promote safe and healthy internet use for families.

Reporting

- It is imperative that any illegal or suspicious contact with a child on the internet is reported to the police immediately.