

# **MILTON ROAD PRIMARY SCHOOL**

## **INTERNET SAFETY POLICY**

Milton Road Primary School's Internet Safety Policy is designed to clarify issues pertaining to filtering and Internet monitoring for the all users of the school network whether adults or children.

### **Filtering**

Milton Road 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 a Protex Internet filtering system is maintained to block material inappropriate to children. Among the items filtered are obscene visual depictions, child pornography, or material harmful to minors. It should be noted that, due to the nature of the Internet, no filtering system can be perfect; therefore the service provided to Milton Road Primary School has the ability to add additional blocked sites or to remove sites found to be inappropriately blocked.

### **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 direct supervision of a teacher or staff member. The E2BN Service provides a monitoring system that can record the Internet sites accessed.

### **Messaging**

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, except within the classroom between the teacher and pupils enrolled in an individual class, or within other schemes approved by the school. Additionally, email accounts provided as part of the County Starz Service are allowed. These accounts are under the direct supervision of an assigned teacher. Milton Road Primary School maintains the right to monitor all messaging on its system.

### **Responsibility**

Each user must take responsibility for his or her use of the computer network and Internet. 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 "ICT Code of Conduct" which is shared with all pupils and displayed by each year group in their learning area.

## **Identification of Pupils on the Web**

Pupils' work published on the web will not be identified by their surnames. 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. Parents who do not wish their child's photograph within a group picture to be used on the school website, are asked to notify the school office in writing.

## **Security**

Milton Road Primary School provides a secure network for the school community through the County Network - E2BN.

## **Confidentiality of Pupil Information**

Personal information concerning Milton Road Primary School pupils will not be disclosed or used in any way on the school website 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.

# **APPENDIX**

## **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 (e.g. Soccer\_Kicks is better than Pretty\_Sally13).

- 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. The worst place is a child’s bedroom.

### **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 libraries. 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.

### **Reporting**

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