

Market Rasen Pre School provides the use of internet facilities, for children and staff. The internet provides opportunities to enhance education by helping with home work, providing information and for the planning of activities.

This policy sets out the use of the internet.

Market Rasen Preschool reserves the right to examine or delete any files that may be held on its system or to monitor any internet sites visited.

- Activity that is found to be unsuitable or that attacks or corrupts other systems is forbidden.
- Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received.
- Use for gambling is forbidden.
- Copyright of materials must be respected.
- Use of the system to access inappropriate materials such as pornographic, racist or offensive material is forbidden. This list is not exhaustive.

Rules for Responsible Internet Use

Staff, Students and Volunteers

- All Internet activity should be deemed appropriate.
- Other user's files will not be accessed without their permission.
- Computers will be used only for agreed reasons.
- USB's will not be used without prior permission.
- Permission will be requested before using the internet.
- E-mail correspondence will be directed only to people who have been approved and messages sent will be polite and responsible.
- Computer files may be checked and the internet sites visited may be monitored.

From September 2019 – EYlog and EYman (EyWorks)

- We are using an online management system called EYman, aswell as a new online learning journal called EYlog, which can be used by all staff on pre school owned tablets and computer only.
- The use of EYlog, is to record children's data, track their development and upload evidence of observations throughout their time with us.
- Staff can only use this system within the setting on a setting owned tablet.
- Internet will be used for this purpose on the shared staff tablets and computer.
- Internet can be used for educational purposes such as researching children's interests. It can also be
 used for watching videos if staff deem appropriate and again for educational purposes as well as for staff
 to complete any e learning training.

All staff must adhere to the above; breech of these could result in disciplinary procedures.

Children

- The setting will work with the parents to ensure they are aware of internet use.
- All internet activity should be deemed appropriate.
- E-mail correspondence will be directed only to people who have been approved and messages sent will be polite and responsible.

- Any unpleasant materials sent to the computer must be reported to the manager.
- The internet sites visited will be monitored.
- We will teach children in a child friendly way about staying safe online, by making sure they know when they
 are on IT equipment they have to have permission from an adult and an adult with them at home and at pre
 school, and through discussion.

Parents

Our policy is accessible to parents to ensure they have an awareness of our online safety procedures and can take a part in promoting online safety within the nursery, at home and in the community.

It is essential for parents and carers to be fully involved with promoting online safety within the setting, home and social environment.

It is therefore advantageous to discuss emerging online safety issues with parents and carers.

All information our practitioners receive on courses, will be passed on to parents and carers through leaflets, booklets and recommended online safety books.

E-safety guides, videos, leaflets or any other resource we find useful, we will share with parents/carers via our facebook page or eylog messaging.

Social networking is hugely popular. Many young people are sophisticated in the way they use social media apps and websites, tailoring their communication for different audiences, and accessing them from a range of devices including smartphones, tablets, and games consoles. But social media, like all forms of public communication, comes with some risks. Not all of these risks turn into actual problems; and if children never face any risks, they never learn how to deal with them. By helping your child understand what the risks are, you can play a big part in preventing them from turning into problems.

- 1. Understand the risks children may need to deal with: What they might see or do:
 - Seeing or sharing of violent, sexual and pornographic content
 - Inaccurate or false information and extreme views
 - Promotion of harmful behaviours including self-harm, anorexia and suicide
 - Over-sharing of personal information
 - Actively or unintentionally getting involved in bullying or hurtful behaviour

Who they might meet:

- People who might bully, intimidate or frighten
- People posing behind fake profiles for:
- Mischief-making
- Sexual grooming and stalking
- Blackmail and extortion
- · Identity theft and hacking

How this could affect them:

- Fear of missing out leading to excessive use or exaggeration
- Getting upset by things they have seen and being uncertain about what to do
- Engaging, or being pressured into engaging in more risky behaviour either by accident or by design
- Developing unrealistic, and perhaps depressing ideals of body image and gender
- Becoming subject to peer pressure or interactions that are intense or too difficult to handle
- Creating an online reputation that may create problems for them in the future

2. Practical tips to help minimise the risks your child might face

It's good practice for apps and websites to have safety advice and well-designed safety features which can make a real difference to how safe your child will be when using them. Work through safety and privacy features on the apps that your child is using, or might use. Make sure they understand the point of these and how to use them.

Don't be put off by believing your child knows more than you: the tools are actually guite easy to manage.

- Ask them to show you which social media apps they use and what they like about them. Talk about how they
 use them and what makes them so engaging
- Explain how you can use privacy settings to make sure only approved friends can see posts & images
- Check if any of their apps have 'geo-location' enabled, sharing their location unintentionally
- Show them how to report offensive comments or block people who upset them
- Check 'tagging' settings so that when others are posting or sharing photos online, your child's identity is not revealed. Also, get people's consent before sharing photos
- Encourage your child to come and talk to you if they see anything that upsets them

•

3. Keep talking and stay involved

In a mobile age, children can't be completely protected, even by the best privacy controls; another child may use different settings. So it's important to keep talking to your child about the implications of social media. Getting a sense of what they think in a useful place to start; you may be surprised by how much thought they may have given to the issues. Encourage your child to think carefully about the way they, and others behave online, and how they might deal with difficult situations.

- People may not always be who they say they are online: how can this create problems?
- Why is it unwise to meet anyone in the real world that you've only ever met online?
- Even if you think your messages are private, remember that words and images can always be captured and broadcast.
- People present themselves differently online do they really look like that? Are they always having that good a time?
- Be aware that screens, and especially being anonymous, can lead people to say things they wouldn't say to someone's face.
- What does being a good friend and a likeable person online look like?
- There can be pressure to be part of a particular group online or to be seen to be following a certain set of ideas
- How can you take a step back and make your own decisions?

Some useful linkswe share with parents are:

bbc.co.uk/cbeebies/grownups/article-internet-use-and-safety bbc.co.uk/cbbc/findoutmore/help-me-out-staying-safe-online childnet.com/sns internetmatters.org nspcc.org.uk/onlinesafety parentzone.org.uk thinkyouknow.co.uk/parents askaboutgames.com

Sanctions

We will follow our disciplinary policy and procedure for dealing with the inappropriate use of ICT both onsite and offsite (where known). The Online Safety policy must operate in conjunction with other nursery policies including Health and Safety, Safeguarding and Child Protection, Confidentiality, Privacy Policy and Whistleblowing Policy.