Madeley Nursery School
Responsible use of ICT and Online / Cyber Safety Policy
June 2022

This policy and agreement will be updated in response to changes in legislation and guidance.

At Madeley Nursery School the safety of children and adults is of vital importance. This includes all aspects of nursery life including when using ICT and internet enabled resources.

This policy aims to:

- Explain how adults and children use ICT and internet enabled devices at nursery.
    - Keeping children safe
    - Addressing cyber bullying
    - Promoting wellbeing and health
    - Supporting the curriculum
- Give advice on protecting personal data online.
- Share advice and links of support for parents and carers to promote safe and reasonable use of ICT in the home
- Guide staff on their responsibilities when using ICT.

Introduction

The following information is taken from Childnet.com

"Ofcom's research has shown that 86% of 3–4-year-olds have access to a tablet at home and 21% have their own tablet.

Children of all ages enjoy using technology. We now see young children going online to play games, talk to family, watch videos, and even learn to use voice enabled tech like Alexa and Siri to find out about their world."

Whilst we acknowledge that the use of technology is part of modern life, we also agree that it is important to balance young children's experiences of using ICT and digital media with real-life, multi-sensory experiences.

The following reflects our approach to using digital media and ICT in the curriculum and is taken from the outcome of research done at Madeley Nursery with partner schools from the UK and Sweden, co-funded by Erasmus+ Programme of the European Union.

"We believe it is important to offer young children opportunity to deepen and constantly elaborate their research of the world that surrounds them, to express and communicate with others what they come to know in a multitude of modes and languages including digital languages. These languages are not separate or taught separately but rather weave together enabling children to express what they know 'in a hundred languages'.

Therefore, we see digital learning as a blended modality, often if not always together with other modes and materials.

We aim to create environments and encounters that respect the curious nature of children, not just as inquisitive explorers but as critical thinkers with a view of the world that is their own but that is constructed in relation to others."

https://wethinkeverywhere.wordpress.com/about-us/our-approach-to-learning/

The nature of rapid and dynamic development in ICT and internet enabled tools and resources means that our approach must be highly vigilant and respond to the current experiences of children and adults. Therefore, this policy will describe principles and approaches which will apply in all circumstances, rather than focusing on practical tools and resources which may become obsolete in this dynamic area of change.

What we do in nursery to keep children safe online:

- Risk assessments are done for the safe use of ICT and internet enabled equipment in nursery.
- Children are always supervised when using all forms of ICT and internet enabled devices.
- Children are not allowed to undertake internet searches on their own.
- Staff check internet resources such as website articles, video, or photographs before showing them to children to ensure that they are suitable, and it is safe to do so.
- The ICT equipment in nursery is supplied and updated by Telford and Wrekin Local Authority with cyber security protocols and software.
- Any issues arising when using ICT and internet enabled devices with children must be shared with a Designated Safeguarding Lead so that risk assessments can be reviewed and updated.
- If staff are concerned about a child's internet access out of nursery, they must share their concerns with the child's parents or carers and the Designated Safeguarding Lead in their 'nest' group.
- Staff encourage children to always tell a trusted grown-up if they are sad or worried about something. These issues are addressed in-line with the nursery's Safeguarding and Behaviour policies.

Cyberbullying

Our response to Cyberbullying is linked to our school Behaviour and Safeguarding policies.

The following is taken from the National Bullying Helpline.

"Cyberbullying is bullying and harassment using technology. This includes trolling, mobbing, stalking, grooming or any form of abuse online.

Cyberbullying is most certainly on the increase - more and more cases are being reported to our helpline by children and by extremely worried parents."

https://www.nationalbullyinghelpline.co.uk/cyberbullying.html

Although it is mostly reported by older children, we must not be complacent in nursery.

In nursery our approaches are:

- To encourage all children to speak out to a trusted grown up, and we develop children's confidence and vocabulary to express themselves.
- For children to know that they shouldn't be called unkind things, be excluded by others, laughed at or belittled and that they should not do it to others.
- Children will be taught about online safety as relevant and as part of the Early Years Foundation Stage Curriculum.
- To give parents and carers up-to-date information about cyberbullying and how to prevent and address it through newsletters and leaflets and via links in this policy on the nursery website.

There is support for parents and carers to keep children safe from bullying and Cyberbullying wherever it happens,

https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/bullying-and-cyberbullying/#

The nursery does have the power to examine children's electronic devices, however due to the age of our children we expect that this would be extremely rare. In this case we would follow the guidance in Appendix 1 to this policy.

Advice and Links to support parents and carers at home

What Is Screen Time?

Screen time does not have any official definition. However, it is generally used to describe any time spent using computers, laptops, smartphones, tablets, iPads and e-readers, games consoles such as Xbox, Play Station, DS, PSP and watching television.

All the experts agree that when you decide to manage your child's use of electronic media the most important factor in achieving this is being consistent in your implementation of whatever rules you decide to lay down and to be a good role model. You are the parent, and it is vitally important that as a parent you model the behaviour that you want to see in your children, including the restricted use of screens.

Action for Children have a useful leaflet about screen time for children:

https://services.actionforchildren.org.uk/media/1325730/fleet-parent-support-advisor-screen-time-leaflet.pdf

Keeping your children safe online at home

On their website at the following link, Childnet.com share 8 top tips that you can put in place at home, to help keep your youngest children safe online.

https://www.childnet.com/help-and-advice/keeping-young-children-safe-online/

If you are worried or suspicious about someone who contacts your child online report them to CEOP.

https://www.ceop.police.uk/safety-centre/

For more information regarding reporting, visit the Childnet Need Help page in the parents and carers section of their website

https://www.childnet.com/parents-and-carers/need-help

We recommend that you always supervise a young child when they are online as they may stumble across something which could worry, upset or confuse them.

Since the internet can be accessed from several devices and many of these are portable, we would advise you to keep family and child devices in a busy part of your home e.g., the living room or kitchen. This makes it easier for you to be involved in their technology use and you are right there to answer any questions and help them.

Young children can be enthusiastic users of technology, but it is vitally important to encourage a healthy mix of online and offline activities. This will improve your child's physical health, wellbeing, self-regulating behaviour and sleep quality. There are some strategies that can be used to help manage the time your child spends online, such as setting time limits or using time limiting tools and designating weekly times to use the internet together.

We also advise removing portable devices from your child's bedroom at night to avoid tiredness and improve the quality of their sleep.

Make use of parental controls and filters which can be used on your home internet,devices, phone networks and online services such as Netflix and YouTube.

Visit the Parents' Guide to Technology on the UK Safer Internet Centre website to find out how to set up controls on a device www.saferinternet.org.uk/parent-tech.

Visit www.internetmatters.org/parental-controls to find out how you can set up controls on your home internet, phone network and online services such as Netflix.

Parental controls will work best in combination with supervision and engagement to help your child understand how to stay safe online. As your child grows and develops, so do their online needs. Therefore you may want to periodically review your parental controls to accommodate this.

Always remember to choose a strong password and do not share it with your child.

Gaming may be the very first way that your child encounters life online and there are lots of online games and apps intended to support their learning and development. When choosing a new game or app for your child the first thing to be aware of is the age rating. Games have age ratings, and these are determined by the game's content. PEGI set these ratings along with content descriptors which indicate if a game contains things like violence, in app purchases or scenes of a sexual nature. Google Play and Windows Store apps are also rated by PEGI and the App Store has age ratings too. It is very important to make sure that your young children are not exposed to this inappropriate content, and we advise you to ensure that they do not see or hear it even if it is being used by older siblings or adults in your home.

You can also proactively find great age-appropriate apps and games for young children to use by filtering by age at Common Sense Media. Common Sense Media is a website which provides reviews and lots of useful information on games, but they also cover films, apps, TV shows, websites, books, and music too. Reading online reviews of games from other parents' experiences is a useful way to highlight potential safety issues like whether the game features inappropriate adverts or bad language.

Here are some free online expert advice pages specifically for parents/carers on supporting their child in the digital world. They offer a range of ideas for staying safe online:

https://nationalonlinesafety.com/wakeupwednesday?page=7

https://www.esafety-adviser.com/latest-newsletter/

https://www.internetmatters.org/about-us/newsletters/

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

https://www.thinkuknow.co.uk/parents/

https://www.saferinternet.org.uk/

https://www.childnet.com/

https://www.vodafone.co.uk/mobile/digital-parenting

Acceptable use of the internet in school

All staff and volunteers are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role in nursery.

We will monitor the websites visited by pupils, staff, volunteers, and visitors (where relevant) to ensure they comply with the above.

Staff should:

- Know the name of the person who has the lead responsibility for online safety in school.

- Be aware of the issues of using the internet, social media etc. And know what they must do if a child or parent approaches them with a concern or issue.
- Be familiar with the school's acceptable use agreement for staff, volunteers, governors, and visitors.
- Regularly change their password for accessing the school's ICT systems.
- Hold all personal data with encrypted storage in line with the nursery Data Protection policies.
- Be familiar with the school's approach to tackling cyber-bullying.
- Identify any areas of online safety in which they would like training / further training.
- Identify areas that they require more knowledge of.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g., asterisk or currency symbol).
- Making sure the device locks if left inactive for a period.
- Not sharing the device among family or friends.
- Ensuring anti-virus and anti-spyware software is installed.
- Keeping operating systems up to date – always installing the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

If staff have any concerns over the security of their device, they must seek advice from the administrator, head or deputy head teacher.

How the school will respond to issues of misuse

Where a staff member misuses the nursery's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The nursery will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive regular refresher training as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure children can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence children to make the healthiest long-term choices and keep them safe from harm in the short term

The DSLs will undertake child protection and safeguarding training, which will include online safety. They will also update their knowledge and skills about online safety at regular intervals.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log is kept by the headteacher.

This policy will be reviewed every year. At each review, the policy will be shared with the governing body through the General Purposes Committee. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because as stated earlier in this policy technology, and the risks and harms related to it, evolve and change rapidly.

Appendix 1

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
  - Delete that material, or
  - Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
  - Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.