

Online Safety Policy



WHY? In this modern digital world, children are interacting with a variety of technologies on a daily basis, both in and out of school, which includes not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. Although the use of these technologies can be significantly beneficial to teaching and learning, there are also potential risks that can place children in danger, due to the Internet being an unmanaged, open communications channel where anyone can publish and distribute information. We want to help our parents and children improve their own understanding of esafety issues so they can learn to use the internet and all digital media in a safe and secure way.

Through e-Safety, we can educate children so that they are **equipped, aware, responsible and safe** when they are accessing online systems anywhere, anytime.

WHAT?

This policy operates in conjunction with Paganel Primary School whole school Behaviour and Child Protection/Safeguarding policies.

Current potential risks children face can include, but are not limited to:

- Bullying via text messaging, email, social networking, etc.
- Misuse of personal information including loss of control over personal images, videos and details.
- Access to inappropriate material of an adult nature including offensive/controversial ideas, images and advice.
- Exposure to explicit material including violence, substance abuse and pornographic material.
- Sexual grooming, exploitation and abuse.
- Viruses, hacking and computer security
- Sexual harassment and sexual violence including online sexual abuse
- Sexting (also known as Youth produced sexual imagery)

HOW?

Planning for Online Safety awareness:

- Online Safety **must** be built into the curriculum and, although discrete sessions are highly valuable and necessary, they should not be not relied upon solely to deliver online safety awareness. (see '365 and I learn schemes and resources')
- Class teachers should plan sufficient opportunities for children to be taught and apply specific skills in using electronic technologies safely and responsibly.
- Online Safety assemblies and Internet Safety day will be delivered whole school. Cyberbullying and use of social media is referenced in lessons on a weekly basis.
- **Delivering Online Safety – lessons/activities should:**
 - Teach children to understand and use new technologies in a positive way to develop safe online behaviours that promote confident users anytime, anywhere.

- Teach children to develop skills to access online systems that do not compromise the safety and security of themselves and that of others.
- Provide regular opportunities for children to practise and apply skills in using electronic technologies.
- Educate children about the potential risks and harmful online behaviours (at age-related level and suitability) including online platforms.
- Give guidance to ensure children feel safe and know how to report any Online Safety violations, both electronically (CEOP) and to adults, in and out of school.

Online activities which are not permitted include:

- Searching, viewing or retrieving materials that are not related to the aims of the curriculum.
- Copying, saving or redistributing copyright-protected material, without approval.
- Subscribing to any services or ordering and goods or services, unless specifically approved by the school.
- Playing computer games or using other interactive 'chat' sites unless specifically approved by the school.
- Using the network in such a way that use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages).
- Publishing, sharing or distributing any personal information about a user (such as: home address; email address; phone number; etc).
- Downloading software and screensavers unless given specific permission by the school.
- Any activity that violates a school rule.

WHO?

School

It is the responsibility of **all** staff to ensure that they use in-school technology safely and responsibly, as agreed via the acceptable use policy.

- Class teachers are responsible for planning and delivering Online Safety awareness (through computing curriculum, PSHE, RSHE).
- The staff member who has encountered an Online Safety violation will investigate and report it to SLT and they will conduct further investigations/get involved if required.
- Digital leaders are responsible for attending meetings, sharing expectations with staff and peers and monitoring technology around school.

Home

Although the technology children use every day can seem a bit daunting and you might worry about the risks your child can face online - such as bullying, contact from strangers or the possibility of them seeing illegal or inappropriate content, it is a highly creative place of amazing opportunities. Children use it to learn, play, socialise and express themselves.

If you are worried about what your children are doing online or just generally want to know, here are some conversation starter ideas from www.childnet.com

- Ask your children to tell you about the sites they like to visit and what they enjoy doing online.

- Ask them about how they stay safe online. What tips do they have for you, and where did they learn them? What is OK and not OK to share?
- Ask them if they know where to go for help, where to find the safety advice, privacy settings and how to report or block on the services they use.
- Encourage them to help. Perhaps they can show you how to do something better online or they might have a friend who would benefit from their help and support.
- Think about how you use the internet as a family. What could you do to get more out of the internet together and further enjoy your lives online.

It is important to remember that the legal age to have an account on most social media, Instagram, Facebook, YouTube, Snapchat, is 13 years old.

Remote Learning

As every child starts Paganel Primary School we provide them with an Office 365 and a J2 account. This means that they are able to access a range of resources from including Microsoft Word, Excel and Powerpoint to help with their learning throughout their time here. In addition, we use this platform for home learning, and remote if necessary. This is monitored using NET Support DNA.

Your child will be given a login card with their details on, which includes a QR code, this can be scanned and your child is taken directly to their account. From here you can see the work they have completed at school as part of their lessons.

Resources for staff and parents

- CEOP (<https://www.ceop.police.uk/safety-centre/>)
- Internet matters (<https://www.internetmatters.org/>)
- Childnet (<https://www.childnet.com>)
- Safer Internet (<https://www.saferinternet.org.uk/>)

Resources for staff

- Computing Curriculum Policy
- Computing Folder on Sharepoint (staff, teaching and learning, Computing)
- '365 and I learn schemes of work and resources' (found on the J2 launch page)