Dear Parent,

Internet Safety

E-Safety is an important part of keeping children safe at Yalding Primary School and is taught to all pupils from Year R to Year 6. Children need to keep safe online at both home and school and we ask that you talk to your children about how they can keep themselves safe and behave appropriately online. It is important that we are all vigilant when children are using the internet and act to ensure they are protected from people who may pose a risk to them. Children can accidently or deliberately be exposed to illegal, unwanted or unpleasant content, comments or activity online and there are steps you can take at home to minimise this risk.

The Golden Rules for e-safety at home

Ground Rules

- Discuss and agree as a family how the internet will be used in your house.
    - Discuss what needs to be kept private online (information, credit card details, photos etc)
    - Decide rules for meeting online friends (such as speaking to a parent, taking an adult with them, meeting in a public place, during the day etc).

Discuss using strong passwords with your child so they understand how they can protect their online accounts. Talk about keeping passwords safe e.g. not sharing them with anyone or using the same password for several accounts. If your child's account is "hacked" or compromised then make sure they change their password and report any concerns or suspicious activity. For more advice on using strong passwords visit https://www.getsafeonline.org/safeguarding-children/protecting-passwords/ or https://www.cyberaware.gov.uk/passwords

Online Safety

- Ensure your internet use is safe and secure and we suggest you use tools to help you
    - Install antivirus software, firewalls and secure your internet connections. Visit your ISP website or www.getsafeonline.org for more information.
    - Consider how safe you are when you're online – shopping, banking etc. Make sure you are aware of online threats (such as scams and hoaxes etc) and how you can protect yourself.
    - Filter unsuitable sites by using parental control software. Most ISPs provide free tools and there are free and purchasable programmes you can install.
    - Always remember that parental control tools are not always 100% effective and sometimes things can get past them, so don't rely on them alone to protect your child.

- o Visit www.saferinternet.org.uk/advice-centre/parents-and-carers for safety information about consoles and devices and www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls or www.internetmatters.org for information about parental controls.

Location

- Be aware of the internet enabled devices in your home and how your children can use them
  - o Where possible, locate computers and laptops in a family area where children's online activity can be monitored or supervised.
  - o Always supervise the use of webcams and any applications or devices which allow voice or video chat.
  - o Be aware that children have access to a whole range of devices such as tablets, music players, games consoles and mobile phones which also allow internet access. It is important that you consider what devices your children have access to and talk about safe and responsible use regularly.

Dialogue

- Don't panic – a positive and open relationship is crucial.
  - o Talk to your child and ask them to show you (or even teach you) how they use the internet and the computer, learn which websites or tools they like to use and why. Learning together can often open opportunities to discuss safe practice with your child. You need to know what your child is doing online much like they would offline.
  - o Make sure your child knows to tell an adult they trust if they see something online that makes them feel scared, worried or uncomfortable.
    - ▪ If your child receives any cyberbullying messages etc keep them for evidence purposes to show to the school or police and report online bullying directly to service providers and websites.
    - ▪ Always ensure your child knows how to block or report another user who may be sending nasty or inappropriate messages or content and encourage your child not to retaliate or reply.
    - ▪ Always report any illegal online activity to the appropriate agency e.g. the Police, CEOP or IWF.
  - o Make sure you and your child know how to use safety tools and features on the websites or apps they use such as privacy settings, blocking and reporting functions
  - o Make sure your child understands that their online actions can have offline consequences e.g. sending nasty or upsetting messages. Ensure your child knows that once an image or video is sent to someone (friend or stranger), they have lost control and anyone can potentially see it.

It's essential that we are realistic – a total ban on access to the internet is unlikely to work and often could mean children hide what they do and are less likely to report problems. Education around safe use is essential to ensure that all members of the school community can benefit from using the internet.

Websites to visit for more information:

www.thinkuknow.co.uk – Visit the "Parent/Carer" Section and use the "Click CEOP" button to seek advice and report online abuse

www.childnet.com   – Visit the 'Know It All' Section for an interactive guide about online safety

www.getsafeonline.org – Free up-to-date Security advice including using complex passwords and managing hacked accounts

www.pitda.co.uk – Parenting in the Digital Age

www.internetmatters.org – Information from the four largest internet service providers (BT, Sky, Talk Talk and Virgin)

www.commonsensemedia.org

www.nspcc.org.uk/onlinesafety - NSPCC's Share Aware campaign provides information for parents about popular social media sites, apps and games.

www.saferinternet.org.uk – Parents guides to safety tools on popular devices and signposts report mechanisms for some websites.

https://parentzone.org.uk/projects/digital-parenting-magazine - Digital Parenting

https://www.kent.police.uk/advice/online-safety/ - Guidance from Kent Police

www.kent.gov.uk/esafety - Guidance from Kent County Council

If you are worried that your child is at risk of harm or a criminal offence has been committed then you can report your concerns to the Police or Children's Social Care. Please do not notify suspicious profiles of your actions, as this could enable them to delete material which might be required for any Police investigations. You can contact Kent Police via 101 or 999 if there is immediate risk or CEOP by visiting www.ceop.police.uk and using the "Click CEOP" reporting button. You can also contact Kent Children's Social Services on 03000 41 11 11, or email: social.services@kent.gov.uk. There is a CEOP button on our website Home page.

Whilst we do not endorse or recommend any of the suggested links, you may find information that could be useful in protecting your child. It must also be noted that no monitoring or filtering system is 100% effective and should not be used in isolation. Parental controls vary depending on the devices you have at home and it is always best to seek advice form your Internet Service Provider. Education around safe online use and behaviour is essential and as a school we have worked across the school, teaching the children about Internet safety through work with the e-Safety Ambassador programme, KCC and Kent Police.

Other websites that you may find useful information on are:

www.net-aware.org.uk

www.google.co.uk/familysafety

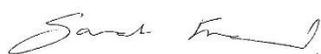https://www.talktalk.co.uk/shop/security/homesafe

We have just developed an IT/e-safety area on our website under the tab 'School Life'. We created a link for 'The Parent Zone' where a digital parenting magazine is published.

The School e-Safety Coordinator (Mr Jason Avards) and Designated Safeguarding Leads (Mrs Sarah Friend and Mr Jason Avards) are happy to discuss any concerns that you may have.

I hope this information is helpful.

Yours sincerely

Mrs Sarah Friend
Head teacher