Staying safe online

- **Online hate (discrimination etc.) and** <u>cyberbullying</u>
- **Outing** – when someone shares private information about someone else without their permission, such as revealing someone's gender or sexual identity online.
- **Doxing/doxxing** – when someone deliberately shares someone's personal identity, such as their real name or address, online without their permission.
- **Personal data collected by apps and devices** – this can sometimes be sold to other companies and misused by them.
- **Privacy** – your personal information could be seen by anyone, anywhere. It could be viewed by friends, family and strangers.
- **Permanency** – once something is posted it can stay online for a long time, even when comments or photos are deleted.
- **Misinformation** – fake news, doctored videos and images and scams can be tricky to navigate online.
- **Grooming** – there are people who try to befriend young people online to have sexual contact. This is against the law.
- **Identity fraud** – people can gather enough information about a person to steal their identity. They can use this to do illegal things like steal your money or commit crimes under your name. It could also be used to create fake profiles to ruin someone's reputation or to bully others.
- **Trolling** – this is when someone misuses social websites to cause conflict or harm an individual or group.
- **Catfishing** – a person can pretend to be someone they're not by stealing a profile or creating a fake one. They can use this profile to trick people over a long period of time.

What you can do to keep safe….

- **Be careful of requests** – only accept 'friend' requests from people you know in real life. This reduces the chance of getting into an unsafe situation.
- **Block anyone you've had contact with that was negative or unsafe** – this stops them from having contact with you and from seeing your profile.
- **Think before you upload and share photos** – post photos that show you and your friends in a positive way. Once it's uploaded, it's no longer private and can be viewed by friends, family, teachers and strangers.
- **Be mindful of what you write to others** – you never know who will read these comments and how they might interpret them.
- **Think carefully about sharing links to other sites** – the content could be embarrassing, upsetting or hurtful to others.
- **Keep your online friends online** – never agree to meet someone you've only known online on your own. Take one of your parents with you and meet in a public place. If they are who they say they are, they'll be happy to do this.
- **Think about your privacy** – avoid sharing personal information online that could be misused by someone in real life. Check your privacy settings and make sure your account is secure.

- **Think critically about online content (link to social post once up)** – not everything online can be trusted.
- **Protect your identity** – pick a username that isn't your real name and a profile picture that doesn't show any personal information.
- **Stay calm** – if you're panicking, take a break.
- **Do some research** – Check out reputable sites that can help, like eSafety and Kids Helpline.
- **Explore your options/problem solve** – normally, there's lots we can do to stay safe and it's NEVER too late to take action.

Get support if needed – talk to a trusted parent, or person in school or report using the studentjusttalk@bosworthacademy.org.uk
The below websites can also support you:
CEOP: www.ceop.police.uk
Child Line: Child Line