Important links:

NSPCC (National Society for the Prevention of Cruelty to Children) – www.nspcc.org.uk

IWF (The Internet Watch Foundation) – www.iwf.org.uk

- To report – https://report.iwf.org.uk/

Internet Matters – www.internetmatters.org

Parent Zone – https://parentzone.org.uk

Common Sense Media – www.commonsensemedia.org/app-reviews

Cyber Security Advice – www.eastmidlandscybersecure.co.uk

Important information:

Passwords – use three random words and special characters – make it long and difficult to guess. For example -Water!PhilosophyZebra$ - Save your passwords in your browser or use a password manager.

2FA – Make sure it's enabled on all accounts.

Digital footprint – Remember that everything you do online leaves a trace.

Social Media – Keep your privacy settings locked down! This includes choosing friends only, turning your location off and checking before you click or subscribe. Check privacy settings on a web browser for more options.

Gaming- Never download from unknown sources. Be careful of people you don't know in real life. Never trust links or instructions from players your child meets online. Remember you can always block and report players.

Spotting the signs or online abuse – Create a safe space and an open environment for your child to speak with you.

Best practice for online abuse:

- Have an open conversation without judgement or shame and talk to your child about online abuse
- Have a family agreement and set out boundaries so everyone can go online positively and safely
- Take interest and learn about the platforms that your child uses
- Know how to use safety tools, apps settings and parental controls

Types of cybercrime –

- Denial of Service (DoS), where multiple requests are sent to a network to shut it down
- Phishing, you will receive an email with a bad link, the aim of this is to steal data or give you malware or ransomware

Verify – if you are unsure, always navigate to a company's website and get the contact details yourself.

Device security – Remember to check software, apps, and antiviruses are up to date

Parental controls – make sure these are turned on and setup correctly!

Important contact details:

Report phishing emails to – report@phishing.gov.uk

Report phishing texts to – 7726 (spells SPAM on your keyboard)

Action Fraud – 0300 123 2040 or online at www.actionfraud.police.uk