**What is Cybercrime?**

 **One Minute Read**

Cybercrime is criminal activity committed using computers and/or the internet. Cyber-dependent crimes include:

 • unauthorised access to computers (illegal ‘hacking’), for example accessing a school’s computer network to look for test paper answers or change the grades awarded

 • ‘Denial of Service’ (Dos or DDoS) attacks or ‘booting’. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources

• making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.  **It is becoming the case that children are being drawn into cybercrime at primary school age.**

Therefore, if there are concerns about a child in this area, the DSL (deputy DSL in their absence) will consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.  Any referral will first be discussed with the parent/carer before the referral is made.

Possible words to look out for:

