

## Policy document for: **Cyber Crime**

Updated: Autumn 2025

*This policy forms part of the Trust Safeguarding and Child Protection policy and gives specific school actions in relation to their context.*

### **Linked guidance**

- Keeping Children Safe in Education

**Staff must remember contextual safeguarding.** When considering safeguarding incident or behaviour concerns, all assessments must consider whether wider environmental factors are present in a child's life that are a threat to their safety and/or welfare. This is an approach to understanding and responding to children's experiences of significant harm beyond their families. This includes online abuse.

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer).

BA MAT schools recognize that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer/internet enabled device) cybercrime.

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 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, and,
- 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.

If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL or a deputy will be informed, and consideration will be given to accessing local support and/or referring into the [Cyber Choices](#) programme, which aims to intervene when children 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.

Where there are concerns about 'cyber-enabled' crime such as fraud, purchasing of illegal drugs online, child sexual abuse and exploitation, or other areas of concern such as online bullying or general online safety, they will be responded to in line with the child protection policy and other appropriate policies.

**Kent DSLs may also seek advice from Kent Police and/or the Front Door Service.**

Guidance:

- [Cyber Choices - National Crime Agency](#)
- [National Cyber Security Centre - NCSC.GOV.UK](#)