Cyber crime (KCSIE 2026)

What staff need to know

Cybercrime is any criminal activity carried out using computers or the internet. KCSIE 2026 requires staff to treat cybercrime concerns as safeguarding issues first, not behaviour problems. Cybercrime falls into two categories:

- Cyber-enabled crime – offline crimes that can be scaled online (e.g., fraud, purchasing illegal drugs, online bullying, child sexual exploitation).
- Cyber-dependent crime – crimes that can only be committed using a computer or digital device (e.g., hacking, DDoS attacks, creating or sharing malware).

Children with strong computing skills may inadvertently or deliberately stray into cybercrime. Staff must be alert to this and respond through safeguarding pathways.

BA MAT recognises that pupils with SEND may experience additional barriers when understanding online risks and may be more vulnerable online. Staff are regularly made aware that children with SEND are at more risk and must take these vulnerabilities into account when assessing risk and planning support. Teachers will provide online safety education appropriate to each child's individual needs and level of understanding.

Examples staff should recognise

- Accessing or attempting to access unauthorised systems ("hacking").
- DDoS/DoS attacks or "booting".
- Creating, sharing or obtaining malware (viruses, spyware, ransomware, botnets).
- Using generative AI or deepfake tools to create harmful, fraudulent or abusive content.

How staff must respond

If you are concerned a child is at risk of cyber-dependent crime:

1. **Inform the DSL immediately.**
2. Do **not** investigate yourself.
3. Record concerns clearly and factually.

The DSL will consider:

- **Early Help / Family Help**
- Diversion via **Cyber Choices** (National Crime Agency)
- Referral to **Kent Police** or the **Kent Front Door Service**
- Multi-agency coordination
- Oversight of filtering & monitoring systems (KCSIE 2026 requirement)

Cyber-enabled concerns

Concerns such as online fraud, drug purchasing, online bullying, child sexual exploitation, or AI-generated abusive images must be managed through:

- Trust Child Protection Policy
- Trust Online Safety Policy
- Trust Filtering & Monitoring Policy

These concerns may indicate wider contextual safeguarding risks.

Filtering & Monitoring (KCSIE 2026 requirement)

Filtering & monitoring systems should be reviewed for effectiveness at least once every academic year. The review should be led by the SLT member responsible for filtering & monitoring, with support from the DSL and IT support. Cybercrime risks sit within this wider online safety landscape.

Key linked guidance

- KCSIE 2026 – Part two: Online safety; Annex A: Cybercrime
- Cyber Choices – National Crime Agency
- National Cyber Security Centre (NCSC)

Bourne Alliance Multi Academy Trust

Policy document for: **Cyber Crime**
Updated: Autumn 2026

This policy forms part of the Trust Safeguarding and Child Protection policy and reflects the latest KCSIE guidance. Keeping children safe in education 2026 (in force from 1 September 2026). See KCSIE 2026, Annex A: Cybercrime, for full details.

Linked guidance

- Keeping Children Safe in Education 2026
- Cyber Choices – National Crime Agency
- National Cyber Security Centre (NCSC)
- Trust Online Safety Policy
- Trust Filtering & Monitoring Policy

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as:

- **Cyber-enabled crime:** crimes that can happen offline but are enabled at scale and speed online.
- **Cyber-dependent crime:** crimes that can be committed **only** by using a computer or internet-enabled device.

BA MAT schools recognise that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into cyber-enabled or cyber-dependent crime. Staff must treat all cybercrime concerns as safeguarding concerns first, not solely behaviour or discipline issues.

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 offences, including those above.

Staff responding to concerns about cyber-dependent crime

If staff are concerned that a child may be at risk of becoming involved in cyber-dependent crime, the DSL or a deputy must be informed immediately.

The DSL will:

- Consider Early Help / Family Help, including diversionary support.
- Consider referral 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 positive use of their skills.
- Assess whether the concern meets the threshold for referral to Kent Police or the Kent Front Door Service.
- Coordinate multi-agency involvement in line with local safeguarding partnership procedures.
- Ensure that cybercrime concerns are recorded, risk-assessed, and monitored.

- Ensure responsibilities relating to safeguarding and child protection, including online safety and understanding the filtering & monitoring systems and processes in place, are explicit in the DSL job description, as set out in KCSIE 2026.

Staff must **not attempt to investigate cybercrime themselves**.

Aspire – SEND and communication considerations

As a specialist SEND setting, Aspire recognises that pupils may face additional safeguarding barriers online and offline. Responses to suspected cybercrime must be child-centred and developmentally appropriate.

- Staff should consider the pupil's communication profile, cognitive/developmental level, understanding of online behaviour and consequences, emotional regulation, and known vulnerabilities. Behaviour alone should not be taken as evidence of criminal intent or full understanding.
- Use the pupil's usual communication supports (for example, AAC, visuals, symbols, signing or a trusted adult) when receiving an initial account. Staff should listen, reassure and record factually, but must not investigate.
- The DSL should liaise with relevant SEND, class or pathway staff and, where appropriate, parents/carers and external agencies when assessing risk and planning support.
- Any restriction on technology should be proportionate and should not unnecessarily remove access to communication aids, assistive technology, curriculum access or agreed reasonable adjustments.

Staff responding to concerns about cyber-enabled crime

Where there are concerns about cyber-enabled crime such as:

- online fraud
- purchasing illegal drugs online
- child sexual abuse or exploitation
- online bullying
- harmful online behaviour
- AI-generated abusive or manipulated images (e.g., deepfakes, nudification apps)

These concerns will be responded to in line with the Trust Child Protection Policy, Online Safety Policy, and other relevant safeguarding policies.

- Staff must speak to a DSL in the first instance.

Filtering & Monitoring (KCSIE 2026 Requirement)

Cybercrime risks sit within the wider online safety landscape. KCSIE 2026 requires schools to:

- ensure a review of filtering & monitoring effectiveness is carried out at least once every academic year
- ensure governors have oversight
- ensure the DSL understands the filtering & monitoring systems and processes in place and supports the designated SLT lead (Tracy Taylor – Assistant Headteacher / Lead DSL).
- include checks that filtering works appropriately on all internet-connected devices in relevant locations, with a record kept of those checks

Therefore this Cyber Crime Policy must be read alongside the **Trust Filtering & Monitoring Policy**, which outlines how the school prevents, detects and responds to harmful online activity. The review should be led by the designated SLT member, supported by the DSL and Primary Technology/IT support. The outcome and any required actions should be recorded and shared through the Trust's governance arrangements.

Multi-Agency Advice

Kent DSLs may seek advice from Kent Police and/or the Kent Front Door Service where criminal offences may have been committed or where there is a risk of significant harm.

Guidance:

- Cyber Choices - National Crime Agency
- NPCC – When to call the police
- National Cyber Security Centre - NCSC.GOV.UK