4th November 2026 - Update regarding Bristol City Council cyber incident

Dear Parents and Carers,

You may have seen media coverage today regarding the cyber attack affecting Bristol City Council's Trading with Schools (TwS) IT network. We wanted to contact you directly to provide some reassurance and clarify the position for the schools receiving this letter.

The data theft concerns schools whose IT systems are maintained by Bristol City Council, rather than schools that receive only internet services from the Council. Your child's school receives internet services only. Based on the information available to us, we have no indication that your child's school's systems have been compromised or that its data has been taken as part of this incident.

Bristol City Council has confirmed that it is continuing to investigate information taken during the wider cyber attack, some of which has subsequently been published online. As part of this work, the Council is establishing which schools may be affected and whether information relating to pupils, families or staff is involved. **Importantly, the Council has advised that at this stage it does not believe your child's school will be impacted by this data theft.**

We appreciate that seeing reports of this nature in the media can understandably cause concern. We therefore wanted to communicate with you directly and reassure you about the information we have at this time.

Amplify Education will continue to liaise closely with Bristol City Council and our Data Protection Officer as the investigation progresses. If we receive any information that changes the current position or indicates that your child's school has been affected, we will communicate with you promptly.

Staying vigilant online
Although there is currently no indication that your child's school has been impacted by the data theft, it is always sensible to remain vigilant online. Bristol City Council has advised families to:

- be cautious of unexpected emails, text messages or phone calls, even if they appear to come from a trusted organisation
- avoid clicking links or opening attachments in messages you were not expecting
- be wary of requests to reset passwords, verify account details, provide personal or financial information, or take urgent action
- use strong, unique passwords and enable two-factor authentication where available
- check online accounts for any unusual activity
- forward suspicious emails to **report@phishing.gov.uk** and suspicious text messages to **7726**. [

Amplify Education, Trust House, Teyfant Road, Bristol BS13 0RF T 0117 462 0499 E info@ampedu.co.uk

Amplify Education is registered in England and Wales, registered company number 08089704

If you have any questions or concerns relating to this incident, please contact Amplify Education at **info@ampedu.co.uk**. We are coordinating enquiries centrally so that families receive consistent and up-to-date information.

We will continue to monitor the situation closely and will contact you directly if there is any change to the information we have received.

Thank you for your understanding.



Kind regards,
Sue Elliott
Chief Operating Officer/Deputy CEO
Amplify Education

Amplify Education, Trust House, Teyfant Road, Bristol BS13 0RF T 0117 462 0499 E info@ampedu.co.uk

Amplify Education is registered in England and Wales, registered company number 08089704