

## Data Breach – Frequently Asked Questions

We do understand that you will have some concerns regarding this. We have put together some answers to staff's questions. We hope that this will answer your concern(s).

### **Where did the breach occur?**

The incident involved an external software supplier contracted by Online SCR, which supports our Single Central Record. Our internal systems, including the SCR platform, remain secure and unaffected.

### **Have all staff been affected?**

No – the breach did not impact all staff members.

### **When did the breach occur, and why am I only being informed now?**

The cyber-attack took place on 31 July 2025. The MAT was notified on 20 August and received details of affected individuals on 26 August. Due to the volume of information involved, and despite treating this as a priority, we were only able to complete the necessary checks and communications by 2 September.

### **What does “only text information was affected” mean?**

This indicates that no documents, images, passwords, or financial data were accessed.

### **I am no longer employed at the school. Why is my data still held?**

The data originated from a third-party provider. We are currently investigating this matter with them.

### **I'm concerned about my personal information being compromised.**

We understand your concerns. Please refer to the guidance provided in our original email and also on this platform for recommended actions.

### **Do I need to let my bank know about the breach?**

Whilst there are no bank account details included in the SCR data, you may wish to inform your bank that you have been subject to a data breach and for them to put a note on the account(s).

### **Why have you contacted the Information Commissioner's Office, how will this be of assistance to me?**

As data controllers, we are required to:

1. Assess risk to data subjects – those with National Insurance numbers, driving licence numbers, or passport numbers face higher potential risk of impersonation for new applications.
2. Notify the ICO within 72 hours if the breach is likely to result in a risk to individuals' rights and freedoms – 9:59 Tuesday 26<sup>th</sup> August.
3. Notify affected data subjects without undue delay if the breach is likely to result in a high risk to their rights and freedoms.
4. Provide appropriate guidance on protective steps they can consider.

### **Why have I received two emails regarding this?**

Unfortunately, those staff who were in the higher risk category were sent out twice – we apologise for this.

If you have further questions or concerns, please email [staffhr@bmat.co.uk](mailto:staffhr@bmat.co.uk) for us to assist you further.