Intradev Cyber Security Attack – Frequently Asked Questions

A data breach has occurred involving data processed by a third party used by the company Single Central Record (SCR). It is a confirmed data breach, not a potential data breach.

Internal RMET systems were not breached. RMET's own network and servers were not compromised.

ABOUT THE DATA BREACH

What has happened?

OnlineSCR's external software supplier, Intradev, was subject to a cyber-attack on 31st July 2025, and the attackers were able to gain access to a particular part of their system and copied data that they found there. This included some data from their systems that Intradev had transferred there.

More information can be found using this link: Intradev cyber attack: SCR teacher data may be 'compromised'

Who has it affected?

This breach has impacted people across RMET and many other organisations nationally, whose DBS data was stored on the OnlineSCR. More information can be found in the above link.

Staff have been affected in different ways and all those affected have been sent an email confirming their data was involved in the breach

When did this happen?

The cyber-attack took place on 31st July 2025. From Intradev's assessment so far, the data that is affected is before 22 May 2025. Therefore, data entered in our systems before this date may be affected.

Have other organisations been affected outside of RMET?

Yes. Many schools and organisations across the country have also been affected. Please see the above link.

How confident are we that only those notified have been affected?

We believe that all those affected have been informed about the data breach – either directly by People Services or by their employer (where they were not originally employed by RMET).

We understand that the breach may have affected some or all of the following information:

- Name
- Phone number
- Date of birth

- Email address
- Postal address
- Place of birth
- National Insurance number
- Passport number
- Driving licence number

It does not include:

- Financial details
- Passwords
- Medical information
- Information on any disclosures (e.g. criminal records)
- Information about protected characteristics (e.g., ethnicity, disability, sexual orientation, marital status)
- Photographs or scanned documents

The information that was accessed was in text format only. No documents or images were affected.

What is RMET doing?

- The company OnlineSCR informed us who was affected by the data breach. We have contacted everyone on their list and have given them advice and support.
- This incident has been reported to the Information Commissioner's Office (ICO).
- We have provided staff with information about keeping safe online.
- We have purchased a support package with Experian so those affected and classed as high risk can sign up to their Identity Plus Account for a 12-month period, giving enhanced protection and peace of mind.
- We will reimburse the cost of CIFAS for those members of staff who have been affected and classed as high risk. This will be a one-off reimbursement to provide added security and reassurance.
- **High risk is where at least one of the following was compromised: National Insurance number, passport number, or driver's licence number.**
- Our Interim COO has communicated previously that we must wait for all outcomes of investigations into the cyber-attack and information will be communicated with you as it emerges. We have no indication from the authorities about the timescales of any investigations.
- Our Interim COO is in the process of liaising with Online Single Central Record to gather reassurances that they are looking into enhancing their risk-mitigation controls to prevent attacks in the future.

REPORTING THE BREACH AND DATA PROTECTION

Does RMET need to report the incident to the ICO?

Yes, we have notified the ICO of the data breach.

SUPPORT FOR PEOPLE AFFECTED

What support is available for those who have been affected?

Access to an enhanced credit checking and monitoring service from Experian is being made available for 12 months. Those affected will receive an email with details of how to access this service.

Sign up to CIFAS to give you added Protective Registration this ensures your personal details are flagged on a secure national fraud prevention database used by banks, lenders, and other organisations. This means:

- **Extra checks on applications:** If someone (including you) applies for credit, a loan, or certain financial products in your name, the organisation will see the Cifas flag and carry out additional checks to confirm the application is genuine.
- **Reduced risk of fraud:** These checks make it much harder for criminals to misuse your identity or open accounts in your name without your knowledge.
- **Peace of mind:** While the extra verification may occasionally cause a slight delay when you make legitimate applications, it provides valuable protection against identity theft.

In short, Cifas Protective Registration acts as an added safeguard to help ensure your identity is not misused, giving you greater security and reassurance in your everyday financial activities.

Advice about what additional steps you can take, and the resources available to help protect you from fraud, are also included in these FAQs.

Who can I contact about the data breach?

STeachen@rmet.org

If my passport and driving licence details have been accessed, should I apply for new ones?

The current advice from Experian is that if you sign up to the Experian Identity Plus service, there is no need to apply for a new driving licence or passport.

The service will work on your behalf should any of your information be fraudulently used. It is at this stage you would report the incident to Action Fraud.

What support will I be offered if my data is used maliciously through this breach? For instance, if someone uses the data to create a new payment from my bank account or creates a credit agreement that negatively affects my credit file?

We are encouraging all those who are potentially affected by this to sign up to the Experian service. The trust has purchased this service, so it is free to those affected for 12 months. It will help you to keep an eye out for any changes that suggest someone is using your data improperly – for instance, you will get an alert if someone sets up a new credit agreement. If you become the victim of fraud, you will be offered help through Experian's caseworker

service to get back on track and sort out your credit file.

In addition, you should look out for any unwanted calls, emails or contact to you directly, including monitoring your bank account. You might find it helpful to talk to your bank now to let them know of the situation. Some banks are able to put in place additional identification verification checks for making/setting up payments, to help keep your money safe.

What can I do to protect myself from fraud?

- Stay alert to unexpected emails, calls, text messages or letters that mention personal details about you.
- Never give personal information to unsolicited callers, even if they seem to know details about you.
- Verify any unexpected contact by calling the organisation directly using their official number.
- Monitor for new applications made in your name:
    - Check your credit report.
    - Look for any new accounts, credit searches, or applications in your name that you did not make.
    - Inform your bank, building society and credit card company of any unusual transactions on your statement.

Useful links and contact numbers

Action Fraud
The government has put together this checklist to help on the steps to take to repair your identity and prevent re-victimisation.

The National Fraud and Cyber Crime Reporting Centre has a wealth of advice and resources on the Action Fraud website:

- www.actionfraud.police.uk
- Call Action Fraud on 0300 123 2040

GOV.UK

- Advice from GOV.UK on the actions you should take if you have shared personal information

Financial Ombudsman Service
If you have lost money because of fraud or a scam – and you are unhappy with how your bank or payment service provider handled things – The Financial Ombudsman Service may be able to help.

- www.financial-ombudsman.org.uk/consumers/complaints-can-help/fraud-scams

General advice

- www.citizensadvice.org.uk
- Call Citizens Advice on 0808 223 1133

To report the theft or loss of post

- Royal Mail web site: www.royalmail.com/report-a-crime
- Or call Royal Mail on 08457 740 740

I have been approached by a journalist to ask me about the breach. What do I do?

Please do not offer any comment and refer them to Sharon Teachen, Interim COO at STeachen@rmet.org.

EXPERIAN IDENTITY PLUS

How do I read my credit report? I have never had one before

If you are not sure where to start, take a look at this guide from Experian.

Your credit report has different sections. For instance, it will show information about you, any credit agreements you have (e.g. your mortgage or with a phone company), your financial connections (e.g. spouses/partners), and details of any missed/overdue payments on credit agreements.

What happens beyond 12 months with the Experian service?

At the end of the 12-month period the individuals will get an email to say their subscription is coming to an end and outlining the options available to them.

How up to date is Experian? For instance, if someone set up a credit agreement today, would they tell me today?

Through your Experian Identity Plus subscription, you will be offered daily alerts as to whether something has changed within your credit report. The subscription also allows you to lock your Experian credit report to help stop fraudsters taking out agreements in your name.

I already have an Experian account, or I have used Experian in the past. What should I do?

When you log into Experian using the code we have given you, and you are using your personal email address, you may be told that you already have an account under that username. In this case, either continue to use your existing account (if you are still paying for it) and let us know that you do not need the code – or create a new account using a different email address.

If you need further assistance, please call the Experian support line on 03444 818182 in the first instance.

Experian asks for a lot of personal data, should I be giving this to them?

When you create the account, you will be asked for your email address as a username, you must use your own **personal email account** because reports from Experian contain your own personal financial information which should not be held in a work email inbox.

You may be asked for date of birth and address so that Experian can identify you, and they may ask you for additional data – for example, your mother's name as an additional security check.

They will already know some of your financial arrangements e.g. mortgage information and bank account details etc, or other financial arrangements where you have had to get a credit check, and they will ask you to confirm these.

Experian needs these details to ensure that it can monitor all your financial arrangements,

however, it also collects data for marketing purposes.

You should read their Privacy Notice here: Experian Consumer Privacy Policy

To opt out of marketing click here: Opt out by marketing channel and industry sector – Experian Consumer Information Portal

Should you have any further questions, please email them to STeachen@rmet.org.