NASUWT THE TEACHERS' UNION

BULLETIN

PROTECTING YOURSELF AFTER THE ONLINESCR/INTRADEV DATA BREACH

You have received this bulletin from NASUWT because your employer has been identified by a company, OnlineSCR, as an employer that uses its services to store personal employee data.

WHAT HAPPENED

OnlineSCR's software supplier, IntraDev, suffered a cyber-attack which led to a breach of personal data. This may have included sensitive details such as names, home addresses and passport numbers. The organisation responsible has reported the incident to the Information Commissioner's Office (ICO), and investigations are ongoing.

As members of the teaching profession, it's important to understand how this may affect you and what steps you can take to protect yourself.

WHAT THIS MEANS FOR YOU

Because this data could be misused, members should be alert to the following risks:

- Phishing emails and texts – Criminals may impersonate official bodies (schools, unions, banks, government agencies) to trick you into clicking links or sharing more details.
- Social engineering calls – Cyber-attackers may phone pretending to be from the union, your school, or even HMRC, using stolen personal details to sound convincing.
- Identity fraud – With passport numbers and addresses, criminals may try to open accounts, apply for credit, or use your identity unlawfully.

HOW TO PROTECT YOURSELF

Stay alert to suspicious contact

- Treat unexpected emails, texts or calls with caution.
- Never click links or download attachments unless you are sure of the sender.
- Verify requests directly, if someone claims to be from your union, school or bank, hang up and call them back using an official number.

Secure your accounts

- Change your passwords on any accounts linked to your school or personal details.
- Use strong, unique passwords for each account.
- Enable multi-factor authentication (MFA) wherever available.

Monitor your identity

- Keep a close eye on your bank accounts and credit files for unusual activity.
- Sign up for credit monitoring services from providers like Experian, Equifax, or Credit Karma. Some providers offer free basic monitoring.
- Report any suspicious credit applications or financial activity immediately.

Take extra care with documents

- Be cautious about sharing scans of passports or IDs online or via email.
- If you suspect your passport number is being misused, you can report it to HM Passport Office.

What to expect next

- Updates from NASUWT – We'll share any new information from the ICO or the affected organisation as it becomes available.
- Guidance from the ICO – The ICO may issue recommendations or require specific actions by the organisation.
- Support for members – We are working to ensure affected members receive clear advice and, where necessary, practical help such as identity protection resources. We will be writing to every employer which contracts with OnlineSCR to outline what the practical measures are which they need to take.

Where to get help

- Action Fraud: Report phishing and scams: **actionfraud.police.uk**
- ICO advice on data breaches: **ico.org.uk**
- Your bank or financial provider if you notice suspicious activity.
- NASUWT – Contact us directly with any concerns or questions: **nasuwt.org.uk**

Please do be aware that 'no-win/no-fee' claims management companies may contact you in respect of a potential legal claim. NASUWT advises caution in this regard as the Union is exploring legal options for members which would enable you to retain all of any compensation to which you would be entitled.