

Reference number: IC-556535-D1K0

I am writing about the personal data breach report you submitted on 19 August 2026. Thank you for the information you have provided.

Section 170 considerations

Section 170 of the Data Protection Act 2018 creates a criminal offence for a person to obtain, disclose, or retain personal data without the consent of the controller. We can carry out criminal investigations where we believe an offence may have been committed and where doing so would be a proportionate use of our regulatory powers.

Our decision

We have determined that opening a criminal investigation would not be proportionate or in line with our enforcement approach. This decision reflects the need to ensure that our resources are directed towards cases where ICO involvement is likely to have the greatest regulatory effect.

Regulatory Action Policy and proportionality

When deciding whether to take forward a criminal investigation, we will apply our [Regulatory Action Policy](#). We will target our resources at matters where our involvement is likely to have the greatest public interest impact. Although we recognise that a loss, disclosure or retention of information can have a significant effect on an organisation, our primary focus will be on protecting the individuals whose personal information is involved.

Our assessment considers the nature of the incident, any evidence of criminal intent, the level of harm that can reasonably be demonstrated, and the steps you have already taken in response to the breach. We recognise that you may view the impact differently, but we must make decisions based on the information available to us and our statutory responsibilities.

Next steps

As this concludes our involvement, you may wish to seek independent legal advice about any steps that may be available to you outside of the ICO's remit.

It is important to note that you remain responsible for ensuring that appropriate internal

policies, controls, and staff training are in place to prevent unauthorised access to, or misuse of, personal information.

We note that you have reported that you do not know whether those responsible for the breach had received data protection training within the last two years. All staff and others who handle personal data on behalf of the organisation should receive appropriate data protection training, regardless of their role, employment status, or any previous training undertaken elsewhere.

Training should be provided as part of the induction process and, where possible, completed within one month of the individual starting their role. Refresher training should then be completed at regular intervals to ensure staff remain aware of their data protection responsibilities.

This training supports compliance with the UK GDPR and the Data Protection Act 2018 by ensuring individuals understand their data protection responsibilities and helping to reduce the likelihood of personal data breaches.

You should continue to take proportionate action to ensure that the personal data obtained without authority, or without a business reason, has been fully recovered. If necessary, you may wish to obtain legal advice to ensure the return or permanent, secure deletion of any personal data retained without consent. Continuing to hold, or refusing to return, personal data without the data controller's permission may constitute a criminal offence under section 170 of the Data Protection Act 2018. You should also consider obtaining written confirmation from the individual, where possible, that they hold no copies of the data and will not share or disseminate it in any way.

In cases such as this, it may be possible for an organisation to take its own action through the courts in respect of contractual breaches. Please note that the burden of proof in civil proceedings, on the balance of probabilities, is lower than the burden of proof in criminal proceedings, beyond reasonable doubt. It may also be appropriate to contact the police in respect of possible offences under the Computer Misuse Act. The police have wider powers in respect of offences of this nature and are the most appropriate body to investigate such matters.

You should also read the attached leaflets, which set out general recommendations and practical steps to help prevent personal data breaches of this nature. If you are not already doing so, you may wish to consider implementing these measures.

If further information comes to light that materially changes the position, we may

reconsider our assessment.

I understand that our decision may be disappointing, but I hope the reasoning set out above explains our position.