From: icocasework@ico.org.uk
To: [redacted]@west-norfolk.gov.uk;
CC:
Subject: ICO Decision - IC-286561-T0C9
Direction: Outgoing
Date Sent: 29/02/2024 16:06

29 February 2024

ICO Reference Number: IC-286561-T0C9

Dear [redacted],

I am writing about the personal data breach report you submitted on 2 February 2024.

Thank you for the information provided.

Data security requirements

It is important to have appropriate technical and organisational measures in place to ensure the security of personal data.

Our decision

We have considered the information provided and we have decided not to take action. This decision is based on the information we have recorded about the breach.

Please note that we may make enquiries if we become aware of new information that affects the circumstances of this case.

We deal with thousands of personal data breach reports each year. In many cases, the breach could easily have been prevented. Please read our attached leaflet, which contains our tips for preventing the most common personal data breaches. If you're not doing these things already, please consider implementing them.

In particular, we recommend that you consider:

- Providing any necessary support to the affected person to help mitigate any potential detriment.
- Reviewing your processes for handling hardcopy documents. This includes the relevant training and guidance provided to staff.
- Introducing a log for hard copy documents. This could include where the documents are being stored and which members of staff handled the documents. This may help you to keep track of documentation. Please see the link for more information on records management and security.
- Reviewing your processes for managing personal data to identify whether documents can be provided by customers via an electronic secure portal. This may allow information to be password protected, encrypted and backed up, which helps to prevent unauthorised access and loss of personal data.
- Reviewing your processes in relation to breach reporting to ensure that data breaches are reported to the ICO within 72 hours of your organisation becoming aware.

Additional information can be provided at a later date. You should have clear processes in place so staff understand the steps to follow to report an incident appropriately.

We also recommend you check that your policies and procedures are fit for purpose. All staff who handle personal data should receive regular data protection training. If you haven't already done so, you should implement any specific steps you identified to prevent a recurrence of this incident.

Thank you for reporting the breach. Further information and guidance relating to personal data breaches under the UK General Data Protection Regulation (UK GDPR) and data security is available on our website at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

We now consider the matter to be closed.

Yours sincerely

Rosina Harrison
Lead Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 ico.org.uk twitter.com/iconews

EMAIL ATTACHMENT COVERSHEET

Attachments included

Attachment Name
Personal Data Security Leaflet - Preventative Measures Local Govt Sector.docx

Attachments excluded

Attachment Name

Personal data security: how to prevent some common personal data breaches in the Local Government sector

1. Always double check

Double check that you are providing the right information to the right people. This applies whether you are providing personal data electronically, by post or in person. Send regular reminders to staff about the importance of always double checking.

2. Add a delay in your email settings

By implementing a 20 or 30 second delay when sending emails, you allow yourself some extra time to check the contents and recipients are correct. If necessary, you can stop the email being sent and prevent a data breach.

3. Disable autofill in your email settings

If people's email addresses come up automatically when starting a new email message, you have autofill enabled in your settings. While this tool might save time, it could lead you to send an email to the wrong person by mistake, so it's a good idea to disable it.

4. Send documents securely

Consider password protecting any documents sent electronically. This can help to keep information secure and prevent it from being accessed by any unauthorised individual. In addition, you should send the password in a separate email or provide it to the recipient over the phone.

5. Treat data in confidence

Not everyone is authorised to have access to or be told about personal data. Only members of staff who are required to use the personal data should have access to it, and they should be careful not to talk about personal data in front of anyone who isn't authorised to know about it. This includes other members of staff or sometimes family and friends of

the data subject. If you're not sure whether someone is allowed to know information, you should double check before informing them.

6. Clearly mark any data handling requests for all staff to see

Some individuals have specific requests about how their data is handled. For example, some may not want their partner or family member knowing certain things about them. You should clearly mark instances like this on an individual's file and take extra care to comply with these requests. For example, this could include being sure to redact an individual's address from documents sent to their ex-partner.

7. Take time to review any redacted documents

Some documents require personal data to be removed before sending. For example, when complying with a Freedom of Information request, a subject access request, or sending confidential documents. Before sending, you should always go back to double check all redactions have been made. Try using the Ctrl-F keys to search for any key words or phrases to ensure they have all been redacted correctly.

8. Make sure your systems are up to date and correct

Whether you are sending out a large amount of letters for a new initiative using a mail merge or using software to redact a document, you should be confident that the systems you are using are working correctly. Check your systems regularly so that any flaws or errors can be identified and fixed before a breach happens.

9. Make sure all staff have received data protection training

Members of staff who handle personal data should receive data protection training regularly, ideally once a year. This training should cover how to process data securely, what to do if a personal data breach happens, and the ways in which each member of staff can keep data security in their mind.

10. Keep your records up to date

Periodically review your records to ensure that all are kept up to date. You should do this by ensuring you have a procedure in place for verifying all personal and contact details are correct. This could prevent you from, for example, sending a letter containing personal data to someone's old

address or leaving a voicemail containing personal data on someone’s old number.