

# **IC-316346-Q1Q3**

Case file for personal data breach IC-313956-  
M2P6 (Jasmine Dental Ltd)

## Email

# Acknowledgement - IC-3...

Regarding

Worked By

Status Reason

S...



Activity Marker



Direction



O...

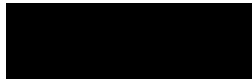


## Email

From

 ICO Casework

To



Cc

Subject

Acknowledgement - IC-313956-M2P6

Display Name

Date Received

19/06/2024 11:26

Email Address

Reference Number IC-313956-M2P6

Dear 

Thank you for contacting the ICO to report a personal data breach. The breach was reported to the ICO on 17 June 2024.

The ICO will use the information you have provided to determine what course of action is necessary. We shall contact you in due course to confirm the outcome.

In the meantime, we would recommend that you read the [security](#) guidance on our website.

If you would like to provide any additional information about the incident reported, please send it to [icocasework@ico.org.uk](mailto:icocasework@ico.org.uk) and enter the reference number in the subject line. This will ensure the correspondence is added directly to the correct electronic case file.

If the person we should contact about this case changes, please let us know.

If we can be of any further assistance please contact our Helpline on 0303 123 1113.

Yours sincerely

Personal Data Breach Service

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

T. 0303 123 1113 [ico.org.uk](http://ico.org.uk) [twitter.com/iconews](https://twitter.com/iconews)


Please consider the environment before printing this email

Please be aware we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the data protection laws and the Freedom of Information Act 2000. You can read about these on our website ([www.ico.org.uk](http://www.ico.org.uk)). Please say whether you consider any of the information you send us is

**confidential. You should also say why. We will withhold information where there is a good reason to do so.**

**For information about what we do with personal data see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice)**

#### ATTACHMENTS

File Name	Followed	File Size (Byte...)	↻
 <p>There are no Attachments to show in this view. To get started, create one or more Attachments.</p>			
0 - 0 of 0 (0 selected)		Page 1	

## Email

# ICO Decision - IC-313956-...

Regarding

Worked By

Status Reason

S...



Activity Marker



Direction



O...

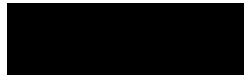


## Email

From

 ICO Casework

To



Cc

Subject

ICO Decision - IC-313956-M2P6

Display Name

Date Received

20/06/2024 08:59

Email Address

20 June 2024

ICO reference number: IC-313956-M2P6

Dear 

I am writing about the personal data breach report you submitted on 17 June 2024.

  
Thank you for the information provided.

**Data security requirements**

You are required 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.

We note that you have conducted event analysis following this breach and provided further training. Taking lessons learned from an incident can help prevent a recurrence.

We recommend you consider what steps your organisation can take to provide support to the data subject. This could include providing advice and guidance, signposting to aid, or assisting with any financial, legal or professional burdens that may have arisen as a result of this incident. The issue of compensation is discretionary to yourselves and you may wish to seek legal advice regarding this.

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.

Article 33 of the UK GDPR states that breaches should be notified to the supervisory authority "...unless it is unlikely to result in a risk to the rights and freedoms of natural persons". Therefore, a data breach that is unlikely to result in a risk to the rights and freedoms of the data subject does not need to be reported to the ICO.

If you think that the breach is unlikely to result in a risk to individuals you should keep an internal record of the breach including what happened, the effects of the breach and remedial actions taken. If new information which affects the circumstances of this breach comes to light, you should reassess the risk and determine whether it becomes reportable at that point.

For help determining how to assess the risk in a data breach please see our guidance on Understanding and assessing risk in personal data breaches. Additionally, you could also use our self-assessment tool which can help you determine whether a breach is reportable to the ICO.

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

Maxine Hinds  
Case Officer  
0330 414 6023

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF


T. 0303 123 1113 [ico.org.uk](http://ico.org.uk) [twitter.com/iconews](https://twitter.com/iconews)

Please consider the environment before printing this email

Please be aware we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the data protection laws and the Freedom of Information Act 2000. You can read about these on our website ([www.ico.org.uk](http://www.ico.org.uk)). Please say whether you consider any of the information you send us is confidential. You should also say why. We will withhold information where there is a good reason to do so.

For information about what we do with personal data see our privacy notice at [www.ico.org.uk/privacy-notice](http://www.ico.org.uk/privacy-notice)

#### ATTACHMENTS

File Name	Followed	File Size (Byte...)	
<a href="#">Personal Data Security Leaflet - Pre...</a>	No	28,467	
1 - 1 of 1 (0 selected)		Page 1	



# Personal data security: how to prevent some common personal data breaches in the Health sector

## 1. Take care when handling written notes or hard-copy files

If your work involves handling physical documents, make sure it's clear exactly how information should be stored or destroyed. This might involve using locked filing cabinets, or shredding information at the end of a shift. Labelling documents properly will also make sure they're not picked up or destroyed by mistake.

## 2. Double-check letters or emails before sending them

Picking up two letters instead of one, or mistyping an email address, are easy mistakes to make if you're working your way through a lot of correspondence. Ask a colleague to double-check that the right letter is in the right envelope, or that an email address is accurate before it is sent.

## 3. Include a return address on your envelopes

If you send a letter and it ends up at the wrong address, the person who receives it by mistake can return it without opening it if you put a return address on the back.

## 4. Disable autofill in your email settings

If people's email addresses come up automatically when starting a new email message then you have autofill enabled in your settings. While this tool might save time, you could be more at risk of sending an email to the wrong person by mistake (especially if email addresses are similar), so it's a good idea to disable it.

## 5. Provide effective staff training

Wherever possible, tailor the data protection training you provide so that it suits the job role of the staff members receiving it. For example, if staff are routinely given access to clinical systems containing personal data, it's likely to be beneficial to include specific reminders about when they're going to be authorised to view certain pieces of information.

## 6. Secure your electronic information

Encourage everyone to lock their screens when they're away from their desks. This helps prevent others from seeing information they're not authorised to see. Also, make sure to use access permissions and passwords to limit who is able to view certain types of personal data. Having the ability to audit your systems to go back and check whether certain information has been accessed is also a really beneficial way of keeping electronic files secure.

## 7. Consider your surroundings

Sometimes it will be necessary to discuss your patients, clients or employees with others. However, you should make sure this happens in a secure environment where you can't be overheard.

## 8. Send electronic documents securely

If you need to send electronic documents, consider encrypting or password-protecting them. This reduces the risk of the wrong person being able to access the documents. Remember to send any passwords by a separate means.

## 9. Protect email accounts

Having secure passwords which are regularly updated, alongside using multi-factor authentication can help to make sure that email accounts aren't at risk of unauthorised access. Regularly deleting the contents of a mailbox can also help to manage storage.

## 10. Keep your IT systems up-to-date

You can reduce your risk of cyber threats, such as attacks on computer systems, by making sure you regularly install security updates. The guidance issued by the National Cyber Security Centre (NCSC) can help you to prepare for and deal with cyber security incidents you may experience. You can find out more through their website: <https://www.ncsc.gov.uk/>

## 11. Ensure the safe disclosure of information when responding to Freedom of Information Act (FOIA) requests

Reduce the risk of disclosing personal information accidentally by ending the use of original source excel spreadsheets when publicly responding to FOIA requests. You should avoid using spreadsheets with hundreds or thousands of rows and invest in data management systems which support data integrity. Staff who use common data software and are involved in disclosing information should receive regular training. See our guidance on [How to disclose information safely](#) for more information.



You could also view our [checklist for public authorities to use for the safe and appropriate disclosure of information](#) which is available on the ICO website.

It is important to note that organisations should continue to comply with their statutory responsibilities under FOIA.