

## Email

# Data Breach Report

Regarding

Worked By

Status Reason

R...



Activity Marker



E... Direction



I...



### Email

From



To

ICO Casework

Cc

Subject

Data Breach Report

Display Name

Date Received

19/05/2023 12:08

Email Address



External: This email originated outside the ICO.

Dear Sir/Madam,

I would like to report a data breach.

Please find attached the filled in report form from the ICO Website.

Thank you for the helpful advice the ICO staff gave us.

Yours sincerely,



City Evangelical Church

### ATTACHMENTS

File Name	Followed	File Size (Byte...)	
<a href="#">report-a-personal-data-breach-for...</a>	No	182,943	

1 - 1 of 1 (0 selected) Page 1



# Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. **Please do not include any of the personal data involved in the breach when completing this form.** For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

## About your report

Please answer the following questions, to help us handle your report efficiently and to better understand our customers.

If you have already spoken to a member of ICO staff about this breach, please give their name:

### Report type

- Initial report – report complete
- Follow-up report – report complete
- Initial report – additional information to follow
- Follow-up report – additional information to follow

(Follow-up reports only) ICO case reference:

### Reason for report – after consulting the guidance

- I consider the incident meets the threshold to report
- I do not consider the incident meets the threshold to report, however I want you to be aware
- I am unclear whether the incident meets the threshold to report

## Size of organisation

- X Fewer than 250 staff  
 250 staff or more

## Is this the first time you have contacted us about a breach since the GDPR came into force?

- Yes  
X No  
 Unknown

## About the breach

### Please describe what happened

The church had a complaints investigation run by an independent organisation for us. A number of different reports were produced - one for the individuals who complained, one for the person who was complained against, one for the church members, one for the commissioners. The original version given to the person complained against contained information that should have been redacted about the person who complained. This unredacted report was given to the individual. We then had a properly redacted version produced which was given to them.

### Please describe how the incident occurred

By accident/oversight.

### How did the organisation discover the breach?

The complainant was asked to check the report and discovered the unredacted content which they did not want sharing.

### What preventative measures did you have in place?

We do have a GDPR and data protection policy and a Data Protection officer.

### Was the breach caused by a cyber incident?

- Yes  
X No

Don't know

### **When did the breach happen?**

Date: September 2022      Time:

### **When did you discover the breach?**

Date:  September 2022      Time:

### **Categories of personal data included in the breach (tick all that apply)**

- Data revealing racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sex life data
- Sexual orientation data
- Gender reassignment data
- Health data
- Basic personal identifiers, eg name, contact details
- Identification data, eg usernames, passwords
- Economic and financial data, eg credit card numbers, bank details
- Official documents, eg driving licences
- Location data, eg coordinates
- Genetic or biometric data
- Criminal convictions, offences
- Other (please give details below)

Please give additional details to help us understand the nature of the personal data included in the breach:

Name of individual, life experiences.

### **Number of personal data records concerned?**

1

**How many data subjects could be affected?**

1

**(Cyber incidents only) If the number of data subjects affected is not known, estimate the maximum possible number that could be affected/total customer base**

**Categories of data subjects affected (tick all that apply)**

- Employees
- Users
- Subscribers
- Students
- Customers or prospective customers
- Patients
- Children

Vulnerable adults

X Other (please give details below)

Church Members

**Describe any detriment to individuals that has arisen so far, or any detriment you anticipate may arise in the future**

Distress to the individual

**Is the personal data breach likely to result in a high risk to data subjects?**

- Yes
- X No
- Not yet known

Please give details

### **(Cyber incidents only) Recovery time**

- We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident
- We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this
- We have determined that we are unable to restore the personal data to the same state it was at shortly prior to the incident, ie backups failed, no current backup, backup encrypted etc
- We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident

### **Had the staff member involved in this breach received data protection training in the last two years?**

- Yes. The staff member complained against has left the organisation.
- No
- Don't know

### **Please describe the data protection training you provide, including an outline of training content and frequency**

We Access CPD accredited training in GDPR.

### **(Initial reports only) If there has been a delay in reporting this breach, please explain why**

There had been a lot of demands on the church, but accept we should have reported this earlier.

## Taking action

### **Have you taken action to contain the breach or limit its impact? Please describe these remedial actions**

Yes. The individual has been asked to delete the unredacted report and a properly redacted version produced and offered to them.

**Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed**

Ensuring GDPR training is done by staff. Improving our practice.

One of my co-leaders had a 90 minute conversation with a member of staff at the ICO gaining advice in good practice.

**Describe any further action you have taken, or propose to take, as a result of the breach**

Implementing the advice from the ICO

**Have you told data subjects about the breach?**

- Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects
- X Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway
- No – but we are planning to because we have determined it is likely there is a high risk to data subjects
- No – we determined the incident did not meet the threshold for communicating it to data subjects

**Have you told, or are you planning to tell any other organisations about the breach?**

- X Yes -
- No
- Don't know

**If you answered yes, please specify**

We sought advice from the network we are part of.

**Are you a member of a UK GDPR Code of Conduct or Certification Scheme, as approved and published on the ICO website?**

- X Yes
- No

If yes:



### **Please confirm the Code/Scheme name**

ICO Data Protection Registration Certificate - your own scheme

### **Are the Code or Scheme's requirements relevant to the breach that has occurred?**

Yes

No

### **Have you informed the relevant Monitoring Body or Certification Body?**

Yes

No

### **Suspicious websites**

If the breach relates to a suspicious website, you can report the website to the National Cyber Security Centre (NCSC). By reporting, you can help stop cyber criminals and protect others online.

The ICO won't see the details of your report to NCSC, so you should make sure you tell us everything we need to know on this form.

[Report a suspicious website - NCSC.GOV.UK](https://www.ncsc.gov.uk)

## About you

### **Organisation (data controller) name**

City Evangelical Church Leeds

### **Registration number**

ZA383693

### **If not registered, please give exemption reason**

### **Business sector**

Church/Charity

## Registered organisation address

Cemetery Road, Beeston, Leeds, LS11 8SX

## Person making this report

In case we need to contact you about this report

Name: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

## Sending this form

### Initial report

If this is your initial report, please send your completed form to [icocasework@ico.org.uk](mailto:icocasework@ico.org.uk), with 'Personal data breach notification' in the subject field.

### Follow up report

If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

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

Please note that we cannot guarantee security of forms or any attachments sent by email.

## What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number.

22 February 2022 – Version 4.0

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our [privacy notice](#).

## Email

# ICO Decision - IC-234278-...

Regarding

Worked By

Status Reason

S...



Activity Marker



Direction



O...



## Email

From

 ICO Casework

To

 [REDACTED]

Cc

Subject

ICO Decision - IC-234278-W3F8

Display Name

Date Received

17/06/2023 09:29

Email Address

**17 June 2023**

**ICO Reference Number: IC-234278-W3F8**

**Dear [REDACTED]**

**I am writing further to your personal data breach report of 19 May 2023 regarding an unredacted complaint form being provided to the subject of the complaint. This incident affects one data subject.**

**Thank you for the information you have 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 you have provided and we have determined that no further action by the ICO is necessary on this occasion.**

**This decision is based on the information we have recorded about the breach.**

**In particular:**

- The number of data subjects affected by this incident is limited to one.
- You have stated that you do not believe this incident to be likely to result in a high risk to the affected data subject.
- Your organisation has taken steps to contain this incident by contacting the recipient and asking that they delete the unredacted report so that an unredacted copy may be provided to them.
- Your report states that you are implementing measures to prevent a recurrence as discussed with a member of ICO staff on our helpline.

## **Recommendations**

However, we recommend that you review the causes of this incident to ensure that you understand how and why it occurred, and what steps you need to take to prevent it from happening again.

In particular, we recommend that you consider:

- Communicating amongst all staff the importance of data security and reiterating the significance of good data protection practice. This should be done frequently, for example by email, internal bulletin or team meetings.
- Highlighting the importance of double checking attachments and recipients when communicating both internally and externally from your organisation. This should be emphasised within your data protection training for staff, and frequent reminders should be issued to ensure that data protection awareness remains embedded in daily tasks.
- Ensuring your organisation has a clear procedure for verifying any documents, particularly those containing potentially sensitive information, prior to them being sent externally. This should include a method for accurately confirming they are appropriately redacted or edited, and could include multiple stages of checks by different employees.

With regards to your query about informing the data subject, the legislation states that you must inform data subjects without undue delay if you believe a breach may pose a high risk to them. If you have not identified a high risk, you may wish to inform data subjects about a breach but you will not be legally obliged to do so. It may be that you are not able to confirm a high risk until you have been able to investigate. We recommend that you take steps to confirm any risk as soon as possible, so that it can be addressed and mitigated quickly.

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

Thank you for reporting the incident. Further information and guidance relating to data security is available on our website.

We now consider this matter to be closed.

Yours sincerely,

Information Commissioner's Office

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...)	Refresh
 <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