PCC Guide – Reporting a personal data breach

Detailed below is a copy of the form you need to complete which includes some suggested text to assist you.

It is designed as a guide and you should take care in answering the questions required.

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

Parishes will need to alter – expected to be fewer that 250 staff

- ○ 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?

Parishes will need to alter – depending on whether they have previously contacted the ICO

- ○ Yes
- ◉ No
- ○ Unknown

About the breach

Please describe what happened

Parishes will need to update with the date they were informed by APCS

On 22nd August 2025 we were notified by Access Personal Checking Services Ltd (APCS) of a significant data breach that has occurred involving data processed by APCS acting as the data processor.

APCS are a Disclosure and Barring Services (DBS) registered umbrella body, providing criminal record checking services to the [insert name of church body] (the controller).

On 17th August 2025 APCS were notified by Intradev, their external software supplier, that a part of their system had been subject to unauthorised access. The incident itself occurred around 31st July 2025. Intradev confirmed that certain files that relate to personal data were copied from their systems. Intradev became aware of the breach on Friday 15 August and provided APCS with copies of the compromised data on Monday 18 August.

APCS' own network and servers were not compromised; however, they have informed us that they have made a data breach notification.

From assessments made so far by APCS, the data that is affected is from 1st December 2024 to 9th May 2025. APCS have processes that obfuscate historic data, for example six months after a check has been completed, and this limits the exposure.

According to the notification from APCS, they do not store details of criminal convictions as these are only revealed on the disclosure certificate.

Please describe how the incident occurred

Unknown. This is being investigated further by APCS.

How did the organisation discover the breach?

Unknown. This is being investigated further by APCS.

What preventative measures did you have in place?

Not applicable. This is not a breach of our systems.

Was the breach caused by a cyber incident?

(•) Yes

( ) No

( ) Don't know

When did the breach happen?

Date: 31/07/25 Time: Unknown

When did you discover the breach?

Parishes will need to alter the date they were informed by APCS

We were notified by APCS on the 22nd August 2025.

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

Data revealing racial or ethnic origin

Political opinions

X Religious or philosophical beliefs

Trade union membership

Sex life data

Sexual orientation data

Gender reassignment data

Health data

X Basic personal identifiers, eg name, contact details

X Identification data, eg usernames, passwords

Economic and financial data, eg credit card numbers, bank details

X Official documents, eg driving licences

Location data, eg coordinates

Genetic or biometric data

Criminal convictions, offences

X Other (please give details below)

Date of birth, National Insurance Number, passport

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

The data affected is text data only. It does not include images or documents.

Number of personal data records concerned?

Parishes need to add the number of data subjects likely to be affected – those who have submitted an application during the affected period

[insert number] data subjects, but the number of records is unknown, we are awaiting further details from APCS

How many data subjects could be affected?

Parishes need to add the number of data subjects likely to be affected – those who have submitted an application during the affected period

[insert number]

(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

Parishes will need to update with the roles of those who applied – for example, volunteers

Categories of data subjects affected (tick all that apply)

X Employees

Users

Subscribers

Students

Customers or prospective customers

Patients

Children

Vulnerable adults

Other (please give details below)

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

Parishes can alter if they are aware of an impact so far, or they might find this wording helpful.

We are unaware of any detriment that has arisen so far.

Possible consequences that could arise in the future could include phishing emails, identity theft and emotional distress.

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

X Yes

No

Not yet known

Please give details

See above

(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

X 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

No

X Don't know.

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

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

Taking action

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

Unknown. We are unable to provide further information regarding this as this was a breach caused by APCS/Intradev.

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

See above.

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

Parishes to update if they have taken any action

We have paused all disclosure applications to APCS.

Have you told data subjects about the breach?

Parish to tick the correct option

Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects

Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway

X 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?

Parish to tick the correct option

- (•) Yes
- ( ) No
- ( ) Don't know

If you answered yes, please specify

Parishes to answer, such as their Diocese

Charity Commission

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

Yes

X No

If yes:

Please confirm the Code/Scheme name

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

About you

Organisation (data controller) name

PCC name

Registration number

Unique number – can be found on the ICO register if unknown

Business sector

Charity

Registered organisation address

PCC address

Person making this report

In case we need to contact you about this report

Name:

Email:

Phone: