26 August 2025

**Data Breach notification: Information and guidance**

Dear Colleague,

On Friday, it was reported that Church of England bodies have been affected by a data breach at Access Personal Services Ltd (APCS), a company who carry out DBS background checks for a wide range of organisations.

**I regret to inform you that you have been named in the report we have received from APCS.** You are one of a number of staff across dioceses and the National Church Institutions who are affected. We understand that the breach affects applications to roles that required a DBS check from 1 December 2024 to 8 May 2025.

**What happened?**

On 31 July 2025, an external software contractor to our data processor Access Personal Checking Services Ltd (APCS) was affected by a cyber-attack. Some personal data on DBS applications has been accessed by unauthorised individuals. APCS provided a report listing the individuals affected on [insert date] having made us aware of the leak on [insert date].

Church of England central systems and diocesan IT systems have not been hacked, and those respective networks are unaffected by this data breach. There is no direct connection between Church of England and diocesan systems and third-party providers.

**What personal information has been leaked?**

We are waiting for more details from APCS. We understand that the breach may have affected some or all of the following information:

* Your name, phone number, date of birth, email address, address, place of birth, National Insurance number, passport number, driving licence number.

It will **not** include:

* Medical information, information on any disclosures, information about your protected characteristics e.g., ethnicity, disability, sexual orientation, marital status.

The information that was accessed was in text format only. No documents, images, passwords, or financial details were affected.

**What can I do?**

* Stay alert to unexpected emails, calls, or letters that mention personal details about you
* Never give personal information to unsolicited callers, even if they seem to know details about you
* Verify any unexpected contact by calling the organisation directly using their official number
* Monitor for new applications made in your name:
	+ Check your credit report – see below for information about the service that will be available to you from Experian shortly.
	+ Look for any new accounts, credit searches, or applications you didn't make.
* For general advice, contact:
	+ Citizens Advice: 0808 223 1133
	+ Action Fraud: 0300 123 2040

**What is being done?**

**The NCIs will be offering you,** via your Diocese, 12 months of free credit and web monitoring services, provided by Experian, one of the UK’s leading credit reference agencies.

The Experian *IdentityPlus* account helps detect possible misuse of your personal data and provides you with identity monitoring support, focussed on the identification and resolution of identity theft. **We strongly recommend that you sign up for the service as it will send you real time alerts, informing you of any changes to your credit report.**

**We will contact you with information about how to access your Experian *IdentityPlus* account.** We are treating this as an absolute priority and anticipate that you will be able to access this service this afternoon.

**What else are we doing**

* This incident has been reported to the Information Commissioner's Office (ICO).
* We have paused all DBS checks with APCS until further notice.

**Next steps**

While there is no guarantee that your information won't be misused, most people affected by data breaches do not experience any problems. The guidance above provides sensible precautions based on what information was accessed.

Please look out for a follow-up email with details about how to access the Experian credit monitoring service. We strongly encourage that you take this up.