

# Responsible information management

Information Management is a key commitment within ACRO. We track and manage the cause of data breaches closely to ensure we are making continuous improvements to our processes and training.

Of the 580,992 transactions across ACRO business areas in 2021/2022, 0.0012% resulted in a data breach. This amounts to 730 data breaches which is a 13.71% decrease compared to the previous year.

All data breaches are risk rated for the safety and wellbeing of the public and to ensure any impact on individuals is minimised. All medium and high risk breaches undergo further analysis to ensure we meet our obligations to data subjects, and therefore we have self-referred five internal breaches, and a further two externally caused, to the Information Commissioner's Office (ICO). To date, all referrals to the ICO have resulted in no further action. All guidance and feedback received in response to referrals is reviewed for methods of implementation.

## Audit

ACRO has an Audit regime that looks at compliance and integrity. Process compliance audits were introduced this year and are a business priority.

The audits seek to address any gaps identified between established processes and governing legislation.

## Case study

### Shoplifting caution deleted following successful force review

Applicant applied for the deletion of a 2009 caution for shoplifting under the grounds of public interest.

The applicant had just turned 18 at the time of the offence. The force reviewed the request and as there had been no arrests since nor had the applicant come to the notice of the police in those 12 years, they agreed that the caution and associated biometrics should be deleted from national police systems.

730

**Total number of breaches**  
13.71% decrease



5

**Number of breaches resulting in ICO referrals**

3

**Breaches with ICO referrals closed**  
including no further action

2

**ICO referral outcomes not yet known**  
ongoing as of May 2022

580,992

total transaction figures for ACRO including 14,499 FPNs

13.71%

decrease in data breaches compared to the previous year

## Case study

### No Further Action deleted but caution remains on PNC

Applicant applied for the deletion of a 2019 caution for using threatening/abusive words or disorderly behaviour and a No Further Action outcome for a Common Assault. Both events were submitted under the grounds of No Crime.

The force reviewed the requests and could find no information to corroborate the chosen ground for deletion. However, they also completed a Public Interest Assessment. It was determined that the No Further Action outcome would be deleted from the PNC. However, the caution would remain as there was still a 'policing purpose' to retain that event.

## Public access to information

### Record deletion

There has been an eight per cent decrease in requests for record deletion this year. In line with the Data Protection Act we co-ordinate this process on behalf of police forces throughout England and Wales.

Applications are assessed on a case-by-case basis and data subjects are duly notified of the deletion of their records. Concerns and subject rights access are a priority for the public access team and are dealt with in accordance with regulations under the Data Protection Act.

We sent 2,109 requests to the relevant police force for review; 1,567 for which we have received decisions. These are broken down as follows:

- 23 part approved
- 503 rejected
- 508 are with forces awaiting a decision
- 533 approved
- 542 are not eligible or no response\*

\*They are requests which are either not eligible for review under the process or the subject did not respond to our request for further information to progress the application and therefore, we cancelled the application.