Joint Information Board

Tuesday 31 March 2026

Commenced at 10.00am via Microsoft Teams

Attendance

Mike Stamp (Joint SIRO/Director of Legal, Reputation and Risk) (Chair)
Scott Bradley (Chief Superintendent Local Policing) (Devon and Cornwall)
Anthony Hart (Superintendent Local Policing) (Devon and Cornwall)
Sarah Bamford (T/Head of Business Change)
Teri Roberts (Strategic Risk Manager)
Graeme Johnston (Information Standards Manager)
Tom Smith (OPCC Scrutiny Manager) (Dorset)
Charles Jagger (GMB Branch Secretary)
Sarah Gillingham (Dorset Union Representative)
Jane Makewell (Specialist Support Coordinator)
Louise Fenwick (Alliance Head of Information Management)
Richard Dixey (Superintendent Specialist Investigations) (Dorset)
Mark Chivers (Chief Technology Officer)
Jo George (Senior Audit Manager)
Oliver Marks (Information Assurance Manager)
Lucianne Pharoah (Information Manager) (Dorset)
Tracey Furbear (Data Protection and Information Sharing Manager)
Phil Rigg (Planning and Performance Manager)
Paul O'Dwyer (Unison Branch Secretary)
Alex Barclay (Specialist Support Coordinator)

Apologies

Jim Colwell (Deputy Chief Constable) (Devon and Cornwall)
Neil Corrigan (Chief Superintendent, Contact Management) (Dorset)
Dan Evans (Chief Superintendent, Local Policing) (Devon and Cornwall)
Richard Scott (Deputy Head of Alliance Information Management)
Matt Longman (Chief Superintendent, Local Policing) (Devon and Cornwall)
Ricky Dhanda (Superintendent, Professional Standards Department) (Dorset)
Jim Richardson (Alliance Head of People)
Fiona Bohan (Performance Analysis Manager)

Guests

Martin Palmer (ICT Technical Security Team Leader) (for item 04/25/44)
Martin Kane (Consultation Manager)
Rod Cates (ICT Digital Engagement Manager) (for item 04/25/53)

02/26/15 Opening and Declaration of Interests [FOIA Open]

Mike Stamp opened the meeting, welcoming members and noting apologies. No declarations of interest, Health and Safety, or equality concerns were raised

02/26/16 Minutes of the meeting Thursday 5 February 2026 [FOIA Open]

The minutes of the previous meeting on Thursday 5 February 2026 were agreed as a true and accurate record.

02/26/17 Action Log [FOIA Open unless exemptions specified below]

a. **Action 261 Information Assurance Quarterly Update (previous minute reference 01/25/08, 02/25/13m and 03/25/28d) [FOIA Closed s.24]**
[This section has been redacted under Freedom of Information Act 2000 Section 24]

b. **Action 263 Information Assurance Quarterly Update - Cyber Security Training (previous minute reference 02/25/16 and 03/25/28f) [FOIA Closed s. 43]**
[This section has been redacted under Freedom of Information Act 2000 Section 43]

c. **Action 264 Information Assurance Quarterly Update - Change Handbook (previous minute reference 02/25/16 and 03/25/28g)**
An update would be brought back to the meeting on 30 June 2026.
Action to remain open.

d. **Action 271 Information Assurance Quarterly Update - AI communication (previous minute reference 03/25/30)**
A policy had been drafted with rigorous references to local and national guidance. A communications strategy had been developed for MS Co-Pilot Chat. The action would be reallocated to Mark Chivers, and an update would be brought back to Joint Information Board on 30 June 2026.
Action to remain open.

e. **Action 279 Information Assurance Incident Management – PPNs (previous minute reference 04/25/43 and 01/26/03h) [FOIA Closed s.24 Safeguarding National Security]**
[This section has been redacted under Freedom of Information Act 2000 Section 24]

f. **Action 284 Information Assurance Quarterly Update - AI communication (previous minute reference 01/26/03e) [FOIA Closed s.24 Safeguarding National Security]**
Activity completed.
Action closed.

g. **Action 285 Incident Management (Data Breaches) Update (previous minute reference 01/26/04) [FOIA Open]**
Activity completed.
Action closed.

h. **Action 286 Incident Management (Data Breaches) Update (previous minute reference 01/26/04) [FOIA Open]**
Additional time was needed to ascertain where the issues lay. Ollie Marks would produce some targeted communications to see if they reduced the breaches.
For action by: Ollie Marks

Action to remain open.

i. **Action 287 Incident Management (Data Breaches) Update (previous minute reference 01/26/04) [FOIA Open]**
Activity completed.
Action closed.

j. **Action 288 Incident Management (Data Breaches) Update (previous minute reference 01/26/04) [FOIA Open]**
Activity completed.
Action closed.

k. **Action 289 Incident Management (Data Breaches) Update (previous minute reference 01/26/04) [FOIA Open]**
A regional training exercise had been discussed at the regional SIROs meeting. Police Digital Services (PDS) would run some sessions. Ollie Marks would progress this action item and bring a paper to the next meeting.
Action to remain open.

l. **Action 290 Incident Management (Data Breaches) Update (previous minute reference 01/26/04) [FOIA Open]**
This would be progressed as Business as Usual (BAU).
Action closed.

m. **Action 291 Server 2012 Status Report (previous minute reference 01/26/05) [FOIA Open unless specified below]**
A discussion was held at minute reference 02/26/21.
Action closed.

n. **Action 292 Review of Information Asset Owner (IAO) Position and Performance (previous minute reference 01/26/10) [FOIA Open]**
Louise Fenwick had liaised with the Head of Learning and Development regarding moving this forward and had drafted a training programme. The action would be updated to provide clarity around the delivery and Mike Stamp would be sent the proposed change.
Action to remain open

o. **Action 293 Review of Information Asset Owner (IAO) Position and Performance (previous minute reference 01/26/10) [FOIA Open]**
The wording for actions relating to minute reference 01/26/10 would be changed once the Chair had agreed to the proposed changes.
Action closed.

p. **Action 294 BWV Integration to Nice Investigate (previous minute reference 01/26/12) [FOIA Open]**
Activity completed.
Action closed.

q. **Action 295 BWV Integration to Nice Investigate (previous minute reference 01/26/12) [FOIA Open]**
Activity completed.

Action closed.

r. **Action 296 Alliance Backup Retention Policy (previous minute reference 01/26/13) [FOIA Open]**
A discussion was held at minute reference 02/26/27.
Action closed.

s. **Action 297 Availability of Data for Disclosure Functions (previous minute reference 01/26/14) [FOIA Open]**
Work continued to establish a task and finish group. The Terms of Reference were in place, and a date was being set for the inaugural meeting.
Action to be closed.

02/26/18 Information Assurance Incident Management [FOIA Closed s.24 Safeguarding National Security]

[This section has been redacted under Freedom of Information Act 2000 Section 24]

02/26/19 Freedom of Information Act (FOIA) Compliance [FOIA Open]

Members received the FOIA Compliance paper provided by Lorna Skinner which updated members on ongoing compliance across both forces as required by the Freedom of Information Act 2000. A marked improvement in performance in 2026 had been noted. Dorset had been released from ICO quarterly monitoring; however, DCP remained subject to oversight.

Nick Franklin joined the meeting.

A number of requests remained open, including approximately 30 cases that required further input before they could close. The team had managed significant demand in recent months and continued to maintain good compliance rates, despite a reduction in staffing capacity. A potential impact on performance was noted by the Board.

Members discussed the analysis set out in the paper, including consideration of whether the identification of the “top three” contributors to delays would support improvement. It was noted that while this may provide some additional insight, it would be difficult to implement reliably and could risk oversimplifying the causes for delays. The importance of a collaborative and supportive approach with departments, rather than adopting a punitive approach, was noted. It was emphasised that delays were often complex and may relate to factors such as workload and the nature of requests.

The Board discussed progress on the publication scheme and noted the key topics and trends could be extracted from the system, although this required careful interpretation as similar queries could produce varied outputs. It was agreed that the approach showed potential but required further envelopment and evaluation, particularly in balancing the effort required against the overall benefit. It was acknowledged that this was not a complete solution and would not address all areas of demand.

Members recognised that the approach could shift issues rather than fix them and that further proactive work was needed in some areas, such as misconduct. It was also acknowledged that some tasks could not be automated and that improvements would take time. It was agreed that this would remain a work in progress and that an informal update would be brought back to the Joint Information Board on 30 June 2026.

Martin Palmer joined the meeting.

The Board welcomed the collaborative approach, noting improved response time and quality.

The Board:

1. Noted the continued progress in relation to compliance rates.
2. Noted the ongoing challenges in relation to timeliness due to delays caused by late, incomplete or inaccurate information being provided.
3. Noted resourcing changes, in relation to the permanent Senior FOI Officer role and vacant FOI Office role, and the impact this is likely to have on performance.

02/26/20 Information Assurance (IA) Quarterly Review [FOIA Open unless specified below]

Members noted the Information Assurance Quarterly Review paper presented by Ollie Marks which provided an update on the accreditation position for both Forces including the Security Assessment for Policing (SyAP), Codes of Connection and Project Assurance. Members discussed the paper with the following highlights noted:

- There was in increasingly challenging cyber threat landscape influenced by global instability and rapid Artificial Intelligence (AI) adoption.
- Devon and Cornwall Police (DCP) had taken a measured approach to AI; however, more risk-tolerant approaches nationally were creating additional exposure, especially within legacy systems.
- Phishing activity increased, notably ahead of national holidays. Force wide messaging in 2026 would be used to increase end user understanding of risk and the need for vigilance.
- SyAP performance maturity rating was reported as above the national average of 2.50, which reflected sustained team effort. It was noted that national baselines were expected to rise to 3, with some areas potentially reaching 2.53, requiring further work and response planning.
- **[This paragraph has been redacted under Freedom of Information Act 2000 Section 43]**
- Police Digital Services (PDS) had begun to address risks incrementally, with 12 areas released to date, and further increases expected.
- Airwave remediation was ongoing with discussions with PDS to complete accreditation. Most national system owners now used SyAP as a tool for measuring cyber security maturity rather than standalone assessments.

The Board discussed the escalation of cyber risks and there was agreement that thresholds should better reflect the threat level. Cost implications and procurement routes were considered, with possible escalation to the Joint Executive Board to identify funding.

The improvement from 1.69 to 2.50 was recognised as significant progress, though future costs remained uncertain, particularly with the anticipated baseline increase. Previous investments, including infrastructure such as towers, were noted, with a need to ensure value and delivery from an IA perspective.

[This sentence has been redacted under Freedom of Information Act 2000 Section 43] There was an agreement that these changes would need to be monitored in detail.

Cyber insurance was discussed, with concerns raised about limited coverage due to legacy systems and exclusions. It was noted that some organisations were moving away from paying ransoms, and further exploration of insurance options was required, given the potential for significant financial impact in the event of an incident.

The Board:

1. Noted the current cyber risk picture.
2. Noted the Security Assessment for Policing (SyAP) position for both Forces.
3. Noted the outline Code of Connection and Project Assurance position.

02/26/21 Information Technology Health Check (ITHC) and Technical Vulnerability Management [FOIA Closed s.24 Safeguarding National Security]

[This section has been redacted under Freedom of Information Act 2000 Section 24]

02/26/22 Data Protection Compliance [FOIA Open]

Members noted the Data Protection compliance paper presented by Tracey Furbear and Gina Berry which provided an update on ongoing compliance across both Forces as required by data protection legislation.

There were ongoing challenges around the timely delivery of Subject Access Requests (SARs) due to staff shortage in the team. Agency staff were expected; however, the process was still at the vetting stage, meaning that less staff in the team trained to deal with SARs. Demands for SARs continued to be high and overtime was being utilised from other teams in the Information Management (IM) department. Tracey Furbear would contact Mike Stamp when the vetting manager had provided a timeline for onboarding agency staff.
For action by: Tracey Furbear

Current figures showed 455 outstanding SARs, which created risks and increased the likelihood of complaints or escalation to the Information Commissioners Office (ICO). The ICO was under increasing pressure and were taking some time to respond to escalation requests, which provided the opportunity to produce an action plan before action was taken.

The Board:

1. Noted the risk on both Force risk registers that related to non-compliance with statutory requirements under data protection legislation.

2. Noted the provided Key Performance Indicators (KPIs) and compliance figures.

The meeting paused at 11.27am and reconvened at 11.35pm.

Jane Makewell left the meeting and Alex Barclay joined.

02/26/23 Review of Information Asset Owner Position and Performance [FOIA Open]

Louise Fenwick updated members on ongoing work to increase awareness of the importance of information management and the responsibilities of information asset owners within the Alliance. The Information Management Department was working with the Learning and Development Department to develop a new approach where information management 'touch points' were regularly scheduled throughout an individual's career journey. For example, a refresher could be offered to newly promoted Sergeants. Additionally, the creation of short, informative videos, made available on Sharepoint, could create more 'self-service' opportunities for staff to upskill and inform themselves at the point of need.

Louise Fenwick would provide a verbal update on the progress of plans to increase awareness of information management within the organisation at Joint Information Board on 30 June 2026, and a paper would be presented on 29 September 2026.
For action by: **Louise Fenwick**

It was noted that there could be an opportunity to include an input on data management at the Senior Leaders' Event taking place in April and Mike Stamp would contact the Staff Office, who were organising the event, to discuss this.
For action by: **Mike Stamp**

02/26/24 Update from Key Meetings [FOIA Open]

a) Technology Board

Mark Chivers provided a brief verbal update and informed members that Technology Board had not met since the previous Joint Information Board. However ongoing significant projects such as Body Worn Video (BWV), the Citizen Portal, Talos and Taser-10 were progressing as expected. PDS had been employed to conduct a review on the capacity and structure of the Information Communication Technology (ICT) Department, and this was expected to commence with data gathering over the next few weeks.

Sarah Bamford provided a verbal update on activities of Joint Strategic Change Board (JSCB) and the Emerging Technologies and Data Assessment Group relevant to Joint Information Board with the following key points noted:

b) Joint Strategic Change Board

Work related to Priority Based Budgeting (PBB) efficiencies was progressing as expected with activities expected to create further demand within the enabling services for affected departments.
Members noted that the launch of Copilot Chat was imminent; the policy had been approved, and the training and communications plan was awaiting approval.

c) Emerging Technologies and Data Assessment Group

Members discussed the need to provide formalised, focussed resources to develop an organisational approach to the use of artificial intelligence (AI) applications and technology within the Alliance. It was noted that some AI products, such as GOODSAM were already in use within the Alliance, and officers and staff were increasingly experiencing the use of AI by partner agencies in various settings which was raising questions around disclosure of information. The need for guidance and assurance for staff and officers around the use of AI was becoming more urgent. Members felt that the move further into AI technology was inevitable and operational benefits and efficiencies could be significant, but that the move needed to be thoughtful and careful with robust governance structures and policies put in place.
Sarah Bamford would explore resources required to develop an approach to the use of AI within the Alliance and present proposals to a future JSCB prior to presenting it at Joint Information Board.
For action by: Sarah Bamford

Members noted that the increased use of AI was a catalyst for refining data governance, emphasising the need to strengthen unstructured data management and record retention protocols to mitigate potential systemic risks. As a paper regarding unstructured data would be presented to JSCB on 7 May 2026 Graeme Johnston would provide feedback on the paper to Joint Information Board on 30 June 2026.
For action by: Graeme Johnston

02/26/25 Independent Inquiry into Grooming Gangs [FOIA Open]

Members noted the Record Retention Requirements for Independent Inquiry into Grooming Gangs paper presented by Graeme Johnston observing the following highlights:

- Following the December 2025 announcement of an Independent Inquiry into Grooming Gangs, the National Police Chief's Council had provided police forces with guidance regarding their retention requirements under the Inquiry, however the Terms of Reference for the Inquiry would be published by the end of March 2026 and to date the onus had been on individual forces to judge what information to retain.
- Dorset had created a 'task and finish group' to ensure the requirements would be met. A representative from Information Management attended the group.
- DCP's Force Record Manager had liaised with the force lead for Operation Beaconport (a child sexual abuse and exploitation operation led by the National Crime Agency) to secure and retain relevant records and create a 'flag' to identify subsequent relevant material on Niche.

- Information Management had temporarily paused all routine disposals of electronic and paper holdings, including Management of Police Information (MoPI) disposals, and developed a communication plan to ensure organisational awareness.
- Mike Stamp would ensure Temporary Assistant Chief Constable Crime, Justice and Vulnerability was aware of the need to establish, at the earliest opportunity, a DCP task and finish group to implement recommendations from the Inquiry. The group would link in with Dorset's similar group.
  For action by: **Mike Stamp**

Andy Bennington joined the meeting.

02/26/26 Information Risk Management [FOIA Open]

Members noted the Information Risk Management paper presented by Phil Rigg which proposed a change of structure to the governance regarding information risk management. Members discussed the paper with the following highlights:

- The current structure of information risk management governance meant that risks were escalated from the Alliance Information Management (AIM) Risk Register and Dorset Corporate Development Risk Register directly to the DCP Force Management Risk Register (FMRR) and Dorset Corporate Risk Register (CRR), bypassing Joint Information Board (JIB).
- Members were supportive of the proposal to create a meeting prior to JIB where the Head of AIM, the Deputy Head of AIM, the Alliance Information Assurance Manager, the DCP Information Standards Manager and the Dorset Information Manager, facilitated by risk practitioners from the Alliance could review current information risks and identify those which should be brought to the attention of the Board. Members of JIB would then have the opportunity to scrutinise the selected risks, along with their internal controls and mitigating actions at the subsequent JIB.
- It was noted that this approach would better inform the Forces' current corporate risk management processes (FMRR and CRR).
- The new meeting would be chaired by the Head of AIM.

The Board approved:

1. That prior to each Joint Information Board, the Head of AIM, the Deputy Head of AIM, the Alliance Information Assurance Manager, the DCP Information Standards Manager and the Dorset Information Manager, facilitated by the necessary risk practitioners, would meet to identify those information risks that need to be brought to the attention of the wider forces at JIB.
2. That JIB would scrutinise the selected information risks as a standing agenda item, whilst acknowledging that any tasking may need to be progressed via other existing force governance structures.

As this would be Phil Rigg's last meeting prior to retirement, members thanked him for his years of service and acknowledged his significant contribution to the work of Joint Information Board.

02/26/27 Alliance Backup Retention [FOIA Closed s.24 Safeguarding National Security]

[This section has been redacted under Freedom of Information Act 2000 Section 24]

02/26/28 Terms of Reference Annual Review [FOIA Open]

The amended Terms of Reference would be presented at Joint Information Board on 30 June 2026. The Strategic Support Hub would provide a copy of the amended Terms of Reference to the Chair in advance of this meeting.

For action by: **Strategic Support Hub**

Date, Time, and Location of Next Meeting

There being no other business the meeting closed at 12.50pm. The next Joint Information Board meeting would be held on Tuesday 30 June 2026 commencing at 10.00am via Teams.