# Joint Information Board

## Thursday 5 February 2026

## Commenced at 10.00am via Microsoft Teams

### Attendance

Mike Stamp (Joint SIRO/Director of Legal, Reputation and Risk) (Chair)
Scott Bradley (Commander, Cornwall) (Devon and Cornwall)
Louise Fenwick (Alliance Head of Information Management)
Fiona Bohan (T/Head of Performance and Analysis)
Richard Scott (Deputy Head of Alliance Information Management)
Graeme Johnston (Information Standards Manager)
Tracey Furbear (Data Protection and Information Sharing Manager)
Kate Bendelow (GMB Branch Secretary)
Jane Makewell (Specialist Support Coordinator)
Steve Lyne (Assistant Chief Constable) (Dorset)
Antony Hart (T/Commander, NEW Devon) (Devon and Cornwall)
Jim Richardson (Head of People HR Operations – Information Asset Owner)
Richard Bullock (Alliance Head of Business Change)
Tom Smith (OPCC Scrutiny Manager) (Dorset)
Sean Walbridge (Alliance Data Protection and Information Sharing Manager)
Paul O'Dwyer (Unison Branch Secretary)
Sarah Gillingham (Dorset Unison Representative)

### Apologies

Jim Colwell (Deputy Chief Constable) (Devon and Cornwall)
Mark Callaghan (Assistant Chief Constable) (Dorset)
Julie Howe (Chief Superintendent – LPA) (Dorset)
Vicky Goodwin (Deputy Head of Corporate Communications & Engagement) (Dorset)
Dave Thorne Assistant Chief Constable (Devon and Cornwall)
Lindsay Dudfield (Detective Chief Superintendent – Commander) (Dorset)
Mark Chivers (Chief Technology Officer)

### Guests

Brent Woodward-Drake (Alliance Information Security Manager) (for minute reference 01/26/04 and 01/26/07)
James Scorey (Project Manager) (for minute Reference 01/26/13)
Andy Bennington (ICT Digital Delivery Manager) (for reference 01/26/05, 01/26/06 and 01/26/13)
Jess Hudson (Senior Data Protection Advisor) (observer)
Esther Lee (Alliance Information Security Manager) (for minute reference 01/26/04 and 01/26/07)
Andy Hull (Project Manager) (for minute reference 01/26/13)
Kaz Duke-Glover (Legitimacy Manager) (observer)

## 01/26/01 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.

## 01/26/02 Minutes of the meeting Wednesday 28 October 2025 [FOIA Open]

The minutes of the previous meeting on Wednesday 28 October 2025 were agreed as a true and accurate record.

## 01/26/03 Action Log [FOIA Open unless exemptions specified below]

a. **Action 261 Information Assurance Quarterly Update (previous minute reference 01/25/08, 02/25/13m, 03/25/28d and 04/25/42b) [FOIA Closed s.24]**
   [This update has been redacted under the Freedom of Information Act 2000 exemption s.24.]

b. **Action 263 Information Assurance Quarterly Update - Cyber Security Training (previous minute reference 02/25/16, 03/25/28f and 04/25/42c) [FOIA Closed s. 43]**
   [This update has been redacted under the Freedom of Information Act 2000 exemption s.43.]

c. **Action 264 Information Assurance Quarterly Update - Change Handbook (previous minute reference 02/25/16, 03/25/28g and 04/25/42d)**
   Richard Bullock would establish what progress had been made in the development of a Change Handbook and would continue work on the project.
   **Action to remain open**

d. **Action 270 Information Assurance Quarterly Update - AI policy (previous minute reference 03/25/30 and 04/25/42g)**
   The strategy had been worked on and was progressing on a day-to-day basis. There were changes that needed to be made to the policy before it was reviewed by the Executive.
   **Action closed**

Kate Bendelow and Paul O'Dwyer joined the meeting.

e. **Action 271 Information Assurance Quarterly Update - AI communication (previous minute reference 03/25/30 and 04/25/42h)**
   The Artificial Intelligence (AI) policy was yet to be signed off; however, a communications plan had been drafted. Once the AI policy had been signed off, the communications plan could be finalised.
   **Action to remain open**

The Chief Technology Officer would complete and formalise the AI Policy to allow the communications strategy to be finalised.
**For action by: Chief Technology Officer**

f. **Action 275 Review of Information Asset Owner Position and Performance (previous minute reference 03/25/34 and 04/25/42l)**
Discussed at minute reference 01/26/10.
**Action closed**

g. **Action 278 Information Assurance Incident Management - security incidents (previous minute reference 04/25/43) [FOIA Closed s.24]**
[This update has been redacted under the Freedom of Information Act 2000 exemption s.24.]

h. **Action 279 Information Assurance Incident Management - PPNs (previous minute reference 04/25/43) [FOIA Closed s.24]**
[This update has been redacted under the Freedom of Information Act 2000 exemption s.24.]

i. **Action 280 Information Technology (IT) Health Check and Technical Vulnerability Management - server upgrade (previous minute reference 04/25/44) [FOIA Closed s.24]**
[This update has been redacted under the Freedom of Information Act 2000 exemption s.24.]

j. **Action 281 Information Technology (IT) Health Check and Technical Vulnerability Management - standalones (previous minute reference 04/25/44) [FOIA Closed s.24]**
[This update has been redacted under the Freedom of Information Act 2000 exemption s.24.]

k. **Action 282 Information Assurance Quarterly (previous minute reference 04/25/45)**
This was being progressed as Business as Usual (BAU).
**Action closed**

l. **Action 283 SmartSTORM Data Volume Project (previous minute reference 04/25/53) [FOIA Closed s. 23]**
[This update has been redacted under the Freedom of Information Act 2000 exemption s.23.]

## 01/26/04 Incident Management (Data Breaches) Update [FOIA Open]

Esther Lee and Brent Woodward-Drake presented the Incident Management (Data Breaches) Update paper and gave an end of year review for 2025. The following salient points were noted by members:

- A total of 1418 incidents were reported in 2025, which showed an increase on 2024's total of 1114. Of that increase, 250 of the incidents were in Devon and Cornwall Police (DCP) and it was thought that Dorset were most likely underreporting incidents.

- Whilst the red, amber, and green ratings of incidents remained static, there was an increase in the severity of the red incidents that had occurred, with eight that met the threshold to refer to the Information Commissioners Office (ICO) against three in 2024.
- Positive progress had been made in meeting the 72-hour time limit imposed by the ICO. Positive feedback had been received from the ICO regarding the swift reaction to breaches and thanks were given to IAO's for their engagement in the process. No enforcement notices had been received by either DCP or Dorset.
- There had been an increase in the amount of physical data breaches, which included loss of electronic equipment and loss of identification (ID) cars, warrant cards or physical access control (PAC) keys.
- Both forces reflected the national increase in ransomware attacks.

Members discussed the potential security issues in third-party supply chains, where other companies were potentially more vulnerable to attacks.

The importance of meeting the 72-hour ICO timeframe was highlighted. Positive feedback had been received from the ICO regarding the swift reaction to breaches. Members were asked to encourage reporting of information security incidents, both cyber and physical, across their teams and to ensure that all officers and staff understood what constituted a security incident.
**For action by:** **All members**

The Board noted the increase in Public Protection Notice (PPN) breaches with discussions held regarding the potential reasons for the high reporting numbers. Although there had been a change in the way PPN breaches were reported, that only accounted for a percentage of the increase. The Board recognised there was an opportunity for some technical fixes to be established to aid improvement; however, the core issues related to poor initial input of information by the user. Steve Lyne and Antony Hart would liaise with the business to encourage accuracy in relation to the inputting of PPNs.
**For action by:** **Steve Lyne and Antony Hart**

During discussions the following actions were created:

- Mike Stamp would liaise with Nikki Leaper and Steve Lyne regarding appropriate opportunities to share best practice in physical and personal security across both forces.
  **For action by:** **Mike Stamp**
- Steve Lyne would liaise with the Superintendent - Strategic Alliance Operations Support – Dorset and invite him to attend Force Security Group meetings.
  **For action by:** **Steve Lyne**
- Esther Lee and Brent Woodward-Drake would investigate any training courses that were available regarding ransomware attacks and report back to Mike Stamp. Any proposals would be brought back to a future Joint Information Board meeting.
  **For action by:** **Esther Lee and Brent Woodward-Drake**
- An alliance wide communications message would be drafted by Louise Fenwick, including a message from Mike Stamp as Senior Information Risk Owner (SIRO) regarding the importance of data quality and information security (cyber and physical) as a whole force consideration.
  **For action by:** **Louise Fenwick**

Members noted the content of the report and the further need for:

1. Information Asset Owners (IAO) to promote information security within their teams.
2. Further work by Information Assurance to address recurring incident types through targeted work with SMTs and specific teams/business areas.
3. Enhanced cyber resilience by embedding Security Assessment for Policing (SyAP) aligned controls, realise the go live of the British Telecom (BT) Security Tower and ensure compliance with PDS blueprints and internal change/accreditation processes.

## 01/26/05 Server 2012 Status Report [FOIA Closed s. 31(1)c Law Enforcement]

[This extract has been redacted under the Freedom of Information Act 2000 exemption s.31.]

## 01/26/06 Information Technology (IT) Health Check and Technical Vulnerability Management [FOIA Open unless specified below]

Members noted the IT Health Check and Technical Vulnerability Management paper presented by Andy Bennington which updated members on the progress of vulnerability management work, crucial to ensuring the Forces' continued compliance with national standards and codes of connection and IT health check mitigation. Highlights from the discussion were as follows:

- Progress was made against the recommendations and as of 19 January 2026, 2,651 of 10,289 devices had been successfully upgraded.
- The Global Rostering System (GRS) was running locally; however, the system needed to migrate to a cloud-based service. This meant an increase in costs and an increase in capability.
- [This sentence has been redacted under the Freedom of Information Act 2000 exemption s.43.]
- The top five Information and Communication Technology (ICT) risks were:
    - Core switches end of life and single point of failure
    - Windows 10 extended support
    - Automatic Number Plate Recognition (ANPR) Router single point of failure
    - Storage Area Network (SAN) migration
    - Microsoft 365 data management and retention policies

The Board expressed concern regarding the vulnerability of standalone computers and the need to mitigate the risks involved in a device not being on the Force network. There was concern that this would open the force to future Distributed Denial-of-Service (DDOS) attacks. However, this risk was somewhat mitigated by using the single online home to manage the website.

Members were cognisant that a Device Firmware Update health check was due and acknowledged that the final outline for the plan was yet to be approved.

Paul O'Dwyer left the meeting.

The top five ICT risks and the mitigations that were in place were discussed and members were asked to ensure awareness across the Alliance when shutdowns were necessary.

## 01/26/07 Information Assurance Quarterly Review [FOIA Open]

Members received and noted the Information Assurance (IA) Quarterly Review paper presented by Esther Lee and Brent Woodward-Drake, which provided an update on the cyber threat risk to both forces, the IA accreditation positions including the SyAP, Codes of Connection and project assurance. It was noted that the SyAP maturity rating stood at 2.50 for both Forces. This was above the current national average of 2.37.

The cyber threat continued to increase across all sectors with it becoming an increasingly frequent event. Third-party supply chains were viewed as a specific threat as they often did not employ the same level of security as forces and could therefore be an easier target. Therefore, the need to encourage a strong security culture, both cyber and physical was critical.

There had been good engagement with senior management teams to understand the Information Asset registers and identify asset owners. Issues with user culture were recognised and the need to change was highlighted, including the use of multi-factor authentication and passwords, and mitigating the risk of phishing attacks.

Antony Hart left the meeting, and Jo George joined the meeting.

The Board were asked to support the creation of an Information Security themed learning programme for roll out across both Forces. The first step was the creation of an organisational needs assessment (ONA) to establish the need for security training for inclusion in the Annual Training plan. The intention was to create a six-to-12-month e-learning programme, which would take a blended learning approach, with short learning opportunities, briefings and comms, including several cyber and physical based subjects alongside existing mandatory training such as Data Protection.

The Board noted the contents of the IA quarterly review, in particular the improvement to the SyAP score, the current cyber threat picture, and the publication of an updated J-P-015 Information Security Policy, J-P-113 Alliance Artificial Intelligence Acceptable Use Policy and J-Pr-035 Copilot Chat Procedure.

## 01/26/08 Freedom of Information Act (FOIA) Compliance [FOIA Open]

Members noted the FOIA Compliance paper provided by Richard Scott which updated members on ongoing compliance across both forces as required by the Freedom of Information Act 2000. The paper highlighted that compliance rates continued to improve, with an average in DCP of 63.1% (compared to 54.8% in 2024 and 58.4% in 2023) and an average in Dorset of 77.7% (compared to 59.6% in 2024 and 63.8% in 2023.) Both forces had the most successful month for compliance in December 2025 (79.7% in DCP and 87.1% in Dorset.)

The Senior FOI Officer pilot had been extended to 11 March 2026. A full review would take place prior to this date.

Both forces had yellow risks on the Risk Register, regarding the timeliness of responding to Freedom of Information Requests and internal reviews.

The Board noted the hard work of the FOI team and thanked them for their efforts.

## 01/26/09 Data Protection Compliance [FOIA Open]

Members noted the Data Protection compliance paper presented by Tracey Furbear and Sean Walbridge which provided an update on ongoing compliance across both Forces as required by data protection legislation. Highlights from the discussion were as follows:

- Both forces had red risks on the Risk Register, regarding the timeliness of responding to Subject Access Request (SAR) requestors.
- Efforts were ongoing to ensure compliance with the logging requirements for automated systems processing law enforcement data that had been established after 6 May 2016. This included oversight of the ICT Applications Portfolio to record if logging is required, compliant or non-compliant. An update would be brought to the Board should assistance with non-compliance be required.
- A force in the region had been the subject of an ICO enforcement notice, so it was essential to remain aware of non-compliance issues.
- There had been an increase in SAR requests with January 2026 being the second highest month ever for both Alliance forces. July 2025 remains the highest with 227 requests across the Alliance.
- Work continued on improving processes where possible, including implementing bots in Niche and STORM and piloting redaction tools.

Members thanked Tracey Furbear and Sean Walbridge for their update and discussed the increase in SAR requests from 2018 when the new legislation had been introduced.

Antony Hart rejoined the meeting.

The Board noted the risk on both Force risk registers that relates to non-compliance with statutory requirements under data protection legislation and the Key Performance Indicators (KPIs) and compliance figures and the mitigating action that was being taken.

The Board broke at 11.32am, reconvening at 11.41am.

## 01/26/10 Review of Information Asset Owner (IAO) Position and Performance [FOIA Open]

Louise Fenwick gave a verbal update on information asset owner position and performance and updated the Board as to the progress of Actions 275 and 283. It was highlighted that asset management was an Alliance-wide responsibility and that a change within the culture of the organisation needed to take place. A training programme around data responsibilities could not be produced in isolation and needed a more formal position from senior leadership to ensuring understanding and compliance.

Members discussed the risk of unstructured data and the difficulty that it creates to comply with SARs and safeguarding requests. There were suggestions that a training programme could be trialled in Dorset before being commenced in DCP. Steve Lyne would liaise with Louise Fenwick as to how Dorset could be used to initiate a training programme.
**For action by:** **Steve Lyne**

It was important for ICT, Business Change and Information Management (IM) to liaise regarding the best way forward.

Antony Hart left the meeting.

The Board requested a change to the wording of the actions to ensure that they properly encompassed the scope of work involved with an update to be brought back to the next Joint Information Board meeting on 31 March 2026.
**For action by:** **Strategic Support Hub**

Asset owners were thanked for their hard work to date and members were encouraged to continue to remind asset owners of their responsibilities and to ensure asset information was kept up to date.

## 01/26/11 Update from Key Meetings [FOIA Open]

**a) Technology Board**

Mark Chivers provided a brief verbal update on the activities of the Technology Board relevant to Joint Information Board. Due to Priority Based Budgeting (PBB) work, there had not been a Technology Board meeting since 15 October 2025. Towers had gone live throughout January 2026, and the security tower would go live on 16 February 2026. Testing documentation would be completed shortly.

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

**b) Joint Strategic Change Board**

Members were made aware that the Single Front Door had been the most significant project to come out of the PBB process. This would streamline the many processes that had been requested of Change. Activity to establish organisational capacity, the priority processes and ownership was ongoing. A pilot was due in April 2026.

Efficiency activity continued with PBB in DCP and Operation Evolve in Dorset with the aim to deliver new ways of working and automating processes. This included a Body Worn Video (BWV) upgrade and link to Digital Evidence Management System (DEMS).

James Scorey and Andy Hull joined the meeting.

Data issues within projects were a growing area of concern and poor-quality data was impacting on other systems.

**c) Emerging Technologies and Data Assessment Group**

There was no activity to be considered from this group as a result of the PBB process.

## 01/26/12 BWV Integration to Nice Investigate [FOIA Open]

Andy Hull and James Scorey shared a presentation regarding the integration of Body Worn Video (BWV) data to Nice Investigate. The following salient points were noted:

- Data issues had meant that the BWV migration project was late in hitting target dates.
- Poor quality legacy data had led to the need for a complete data review of the entire Reveal BWV platform. Issues included incorrect reference numbers, footage saved with no identifiable force and not booking out the camera correctly.
- 4.9 million records in Reveal had been examined and categorised. Of these, 1 million contained data. There were 181,000 records that had no matching Niche occurrence and could not be attributed to either Alliance force. 118,000 of these were recorded by DCP officers and 32,700 by Dorset officer, which indicated likely ownership. However, 30,700 had no force attributed, no Niche occurrence number and no collar number. The issue of how to process this data has arisen.

The Board discussed the recommendations at length. It was noted that the supplier for BWV may change and this would cause additional issues. Members were broadly supportive of the Review, Retain, Delete (RRD) model proposal to review this data. Reviewing this data manually would have a higher impact on resources and would have a higher error rate.

Andy Bennington left the meeting.

Members agreed that a decision needed to be made regarding the use of the RRD engine to direct the migration of data from Reveal to Nice. The capacity for further manual instigative work before migration was limited, with overtime already needed to manage daily demands.

Andy Bennington rejoined the meeting.

The Board acknowledged the recommendations for the unmatched data and discussed the three options: a comprehensive review ahead of deletion, a light touch review ahead of deletion or deletion without review. BWV cameras were shared across the Alliance, meaning metadata was not helpful in establishing ownership. Members considered that the Digital Evidence Management System (DEMS) Project Board needed to further discuss the options with the BWV asset owners.

The Board:

1. Noted the decision made by the Digital Evidence Management System (DEMS) Project Board on 24 October 2025, which was to manage all BWV footage through Nice Investigate.
2. Noted the supplied Reveal Data Review.
3. Noted the decision made by the DEMS Project Board and endorsed by the SIRO that the Nice review, retain, delete (RRD) model will replace the existing deletion process in Reveal.
4. Approved the migration of unassigned data from categories 1.1, 1.2 and 1.3 from Reveal to Nice Investigate Using the RRD engine to manage this with no updates to retention periods.

During discussions the following actions were created:

- Richard Scott and Rich Bullock would liaise to clarify the process involved in changing to a new BWV supplier and how the DEMS project Board could approach this.
  **For action by:** **Richard Scott and Rich Bullock**
- Mike Stamp would liaise with the Assistant Chief Constable (Vulnerability and Crime, DCP) and the Deputy Chief Constable (DCP) to establish a standalone project board to move forward with the issue of review and deletion of unmatched data.
  **For action by:** **Mike Stamp**

## 01/26/13 Alliance Backup Retention Policy [FOIA Open]

Andy Bennington presented the Alliance Backup Retention Policy on behalf of the ICT Hosting Manager, which outlined the need to update the Force's backup retention policy to clarify the purpose of backups versus archives and emphasise the role of application and records management teams in managing retention requirements within each system.

Jim Richardson left the meeting.

The paper clarified the Force's process for retaining data with the aim of formalising the new procedure as policy. This included keeping data for three months to allow live systems to be restored if necessary. This was a reduced amount of time from the existing practice.

Members noted that the more data that was kept as back up meant the more secure storage solutions had to be sourced and funded. It was acknowledged that retaining data longer than necessary could also increase data protection risks.

During discussions the following action was created:

- Andy Bennington would liaise with Louise Fenwick to establish possible risks in reducing the retention period to three months and bring back an update to the JIB meeting on 31 March 2026.
  **For action by:** **Andy Bennington**

## 01/26/14 Availability of Data for Disclosure Functions [FOIA Open]

Members received and noted the Availability of Data for Disclosure Functions paper presented by Graeme Johnston, which highlighted two elements: the lack of visibility and availability of Access Control Level (ACL) information within Niche Record Management System (RMS) and the data held within Professional Standards Department (PSD) databases, and the way that ACL data was processed by Niche.

The Board heard the request to establish a task and finish group that would be tasked with reviewing working practices and work with PSD to have visibility of key databases.

The Board:

1. Noted the position and risks regarding the lack of availability and accessibility of ACL data within Niches and the PSD databases.

2. Agreed to the establishment of a task and finish group to review working practices and access to DCP PSD databases.
3. Agreed that a review of Niche RMS ACL procedures and configuration for both forces was undertaken to ensure that relevant disclosure and decision-making functions can identify if ACL information exists on restricted records.

During discussions the following action was created:

- Graeme Johnston would establish a task and finish group and request that they undertake a) a review of working practices and access to DCP PSD databases and b) a review Niche RMS ACL procedures and configuration to ensure that relevant disclosure and decision-making functions can identify if ACL information existed. An update would be brought to the JIB meeting on 31 March 2026 to include the flagging of appropriate milestones.
  **For action by:** **Graeme Johnston**

## Date, Time, and Location of Next Meeting

There being no other business the meeting closed at 1.05pm. The next Joint Information Board meeting would be held on Tuesday 31 March 2026 commencing at 10.00am via Teams.