**NORTHERN IRELAND POLICING BOARD**

**MINUTES OF THE SPECIAL MEETING OF THE NORTHERN IRELAND POLICING BOARD HELD ON THURSDAY 10 AUGUST 2023 AT 10AM IN JAMES HOUSE, BELFAST**

| | | |
|---|---|---|
| **PRESENT:** | | Ms Deirdre Toner (Chair) |
| | | Mr Edgar Jardine (Vice-Chair) |
| | | Dr Janet Gray |
| | **(1)** | Mr Mukesh Sharma |
| | | Ms Joanne Bunting MLA |
| | | Mr Maurice Bradley MLA |
| | | Mr Trevor Clarke MLA |
| | **(2)** | Mr Les Allamby* |
| | | Mr Gerry Kelly MLA |
| | **(3)** | Mrs Linda Dillon MLA |
| | | Mr John Blair MLA |
| | | Ms Nuala McAllister MLA |
| | | Mr Frank McManus |
| | | Mr Mike Nesbitt MLA |
| | | Mr Mark H Durkan MLA |
| **POLICE SERVICE OF NORTHERN IRELAND IN ATTENDANCE:** | **(4)** | Mr Simon Byrne, Chief Constable |
| | **(4)** | Mr Chris Todd, Assistant Chief Constable |
| | **(4)** | Mr Bobby Singleton, Assistant Chief Constable |
| | **(4)** | Ms Aldrina Magwood, Assistant Chief Officer, Strategic Planning and Transformation |
| | **(4)** | Mr Stephen Wright, Chief Superintendent, Interim Head of HR |
| | **(4)** | Ms Leanne Barnett, Strategic Communications & Engagement |
| | **(4)** | Two PSNI Officials |
| **POLICE FEDERATION FOR NORTHERN IRELAND IN ATTENDANCE:** | **(5)** | Mr Liam Kelly, Chair* |
| **THE NORTHERN IRELAND PUBLIC SERVICE ALLIANCE (NIPSA) IN ATTENDANCE:** | **(5)** | Ms Tracy Godfrey, Official* |

| | |
|---|---|
| **NORTHERN IRELAND POLICING BOARD OFFICIALS IN ATTENDANCE:** | Mrs Sinead Simpson, Chief Executive<br>Mr Adrian McNamee, Director of Performance<br>Ms Jenny Passmore, Director of Partnership<br><br>Four Board Officials |
| **OTHER OFFICIALS IN ATTENDANCE:** | Mr John Wadham, Human Rights Advisor |

**(1) Left at 11.50am**
**(2) Left at 11.30am**
**(3) Left at 12.30pm**
**(4) Item 3 only**
**(5) 10.20am to 10.35am only**

*Attended meeting by video conference facility

## 1. APOLOGIES

Apologies were received from Mr Peter Osborne, Dr Kate Laverty, Mr Brendan Mullan and Ms Liz Kimmins MLA.

## 2. CONFLICTS OF INTEREST

No conflicts of interest were declared.

The Chair advised Members that a special meeting was called today to allow the Board as the independent oversight body for PSNI to engage with and question the Chief Constable and the PSNI Leadership Team on the significant data breach which occurred on Tuesday 8 August 2023 and the circumstances in respect of a further data breach announced publicly on Wednesday 9 August 2023. This will include an update on actions being taken following the formation of a high level 'Gold' Group to manage this critical incident.

Members then discussed the key issues arising from the data breach and outlined questions and concerns to put to the Chief Constable and the leadership team when they joined the meeting.

The Chair welcomed staff association representatives from the Police Federation for Northern Ireland (PFNI) and the Northern Ireland Public Service Alliance (NIPSA) to the meeting to express their concerns on behalf of Police officers and Police staff in PSNI.

The PFNI Chair thanked Members for the opportunity to outline the impact of the data breach on Police officers and raised the following matters:

- Anger, worry, and vulnerability felt by Police officers at this time, and in particular the impact on those officers working in more sensitive roles,
- Recognition and appreciation that support mechanisms for officers and families have been quickly put in place,
- Long term implications of data breach as information is in the public domain and unlikely to be recovered, and concerns regarding the extent to which data has been shared online and across messenger platforms,
- Hierarchy of risk with officers' personal safety impacted to a lesser or greater extent based on a range of factors including public profile, community background, job role/location, and need for PSNI to ensure all officers affected are kept safe,
- Consequences of the data breach will be felt over the long term and a substantial amount of work is now required to rebuild officer trust and confidence in the organisation.

The NIPSA representative also thanked Members for the opportunity to outline the impact of the data breach on Police staff and raised the following matters:

- NIPSA Members are extremely concerned and upset by this data breach and appreciate the ongoing work by PSNI to allay fears for personal security,
- Police staff also perform front line roles in the community and now feel exposed and at risk following this breach,
- Police staff receive an additional £580 environmental allowance per year compared to around £3500 for Police officers but NIPSA considers the threat level to be the same for Police staff and will continue to lobby the Department of Justice to bring about parity in this area.

The Chair thanked the PFNI Chair and the NIPSA Official for their contribution and they left the meeting.

## 3. PSNI UPDATE ON DATA BREACH

The Chair welcomed the Chief Constable, Assistant Chief Constable Chris Todd, Assistant Chief Constable Bobby Singleton, Assistant Chief Officer Aldrina Magwood and Chief Superintendent Stephen Wright to the meeting.

The Chair provided opening comments noting that many officers and staff will be deeply concerned by this very serious data breach and that Members have just heard the views of representatives from Staff Associations including the Police Federation and NIPSA.

The Chair advised the Board is extremely concerned about the safety of officers and staff, actions which are being taken to support officers and staff to mitigate current and future security risks, and the level of support provided to individuals from the PSNI team directly involved in the data breach.

The Chair also welcomed a fulsome account of the breach to include how it happened, details of plans to carry out an end to end review, managing the impact on officers and staff, the communications strategy in place across the

organisation, assurances that contributing factors and corrective actions have been implemented, whether a series of security breaches this year is indicative of wider cultural issues, and implications in respect of financial liabilities including fines and compensation payments.

The Chief Constable began by outlining the role and responsibilities of the PSNI Leadership team as part of a coordinated response to this unprecedented data breach.

The following briefing was then provided in respect of the PSNI data breach:

- Overall concerns in respect of officer and staff welfare and actions being taken following this serious breach of trust,
- Current communication strategy including regular briefings across the organisation to provide updates and support available from key stakeholders including UK government,
- Financial consequences of the breach which may include compensation for officers and staff affected and penalties levied by the Information Commissioners Office (ICO),
- Details of a further data breach, preceding this breach, relating to equipment stolen from an officer's car and insight regarding the delay in reporting the previous incident to the Board.

A Member thanked the Chief Constable and his team for attending today's meeting at such short notice and noted with regret that not all Members of the PSNI Leadership team were able to attend.

ACC Todd, as PSNI Senior Information Risk Owner (SIRO), and with Gold responsibility for this incident, provided Members with a detailed briefing on the data breach, classified as Operation Sanukite.

The Briefing covered the following key points:

- Details of the initial Freedom of Information (FOI) request and processing timeline,
- Explanation of circumstances leading to the data breach and timeline of events,
- Sample spreadsheet and details of material released,
- Immediate actions taken and ongoing response – communication and support to officers and staff and the establishment of an Emergency Threat Assessment Group,
- Investigations – Criminal and ICO, as well as an independent review by City of London Police, and "lessons learnt" report to be prepared by PSNI Information Security Unit (ISU),
- Arrangements in place in respect of governance, policy, training, audit & inspection, with support from partner agencies.

ACC Singleton provided an update on actions taken to address the impact of the data breach on officers and staff. ACC Singleton advised that along-side established threat management processes a new Emergency Threat Management process had been established to respond to the heightened concerns owing to the unique challenges due to the nature and scale of the breach.

The Emergency Threat Assessment Group has a "triage" function as a single means of communication for officers and staff to raise concerns for a variety of reasons including previously being under threat, community background, family circumstances, and easily identifiable names. At this time additional resources have been deployed to provide necessary supports for those officers and staff for whom it is deemed necessary.

ACC Todd provided a further update on actions taken in respect of processing FOI requests and lessons learned including a change in the format in which FOI's are issued.

ACC Todd noted the additional work taking place in respect of communications to officers and staff including the 'triage' system for individuals to raise concerns as part of the Emergency Threat Assessment Group.

Other arrangements in place in respect of governance processes include a dedicated Data Protection Officer, and experienced Heads of Branch for Information Security and Corporate Information are in place, supported by fully trained teams.

In respect of policy arrangements in place, updates were provided on data storage and handling, the strict adherence to comprehensive checklists, and that data released as part of future FOI responses will be in pdf format only. Training updates provided included an overview of education and awareness programmes in place, and mandatory data protection e-learning to be completed by all officers and staff.

In addition to the above the PSNI Leadership team addressed a range of matters from Members concerning:

- Further clarity in respect of FOI process and reasons for the failure of defined checks and balances.
- Whether the expeditious response to the FOI request given a statutory response window of 20 days was a contributing factor for the breach.
- Role of ICO in auditing responses within the statutory timeframe versus auditing FOI process.
- Training needs to be identified and addressed due to a failure in management to protect highly confidential spreadsheet data.
- Whether this was a systemic breach rather than human error and whether similar data breaches of a lesser extent have occurred in the past, and if so, what remedial actions were implemented including training and development.

- Extent to which other unrelated confidential datasets exist and processes in place in respect of security, encryption and user access.
- Serious concerns in respect of the extent to which data released as part of FOI response can be manipulated by member of public after downloading.
- Reasons why information not relevant to FOI response were copied over to spreadsheet and not deleted immediately, for example, surname, initial, location.
- Clarity in respect of FOI process and grade of senior HR member authorised to approve information for release, processes and checklists in place before and after data released, and direction provided to officers regarding equipment and data handling in public places relating to a separate data breach in Newtownabbey.
- Timeline of separate data breach in Newtownabbey and reasons for delay in escalation to the Board.
- Extent to which PSNI has the resources to manage the impact of this data breach, and scope for proactive reach in to staff and officers to complement the reactive strategy where officers and staff can flag concerns as part of a triage system.
- Concerns regarding the financial cost to PSNI in respect of fines and compensation, and impact of the data breach on intelligence gathering and confidence in PSNI going forward.
- Extent to which confidential data was downloaded from FOI website and how a root and branch review of current data management processes was needed.
- Concerns expressed regarding previous security breaches, lack of management control, and what can be done to improve compliance and restore pride in the organisation.
- Need to ascertain full extent of risk to officers and staff concerned and likely impact of breach on welfare, morale, work location, and reassurance that all of those affected receive regular and effective communication.

- Board Members assured that failsafe systems will be put in place and any future incidents will be communicated to the Board as a matter of urgency and Members will be kept fully informed.
- Recognition that events have moved at a fast pace during the week and unfortunately some Members of the PSNI Leadership team were unable to join the meeting.
- Whether a data breach of this nature is currently recorded on the PSNI risk register.
- Mechanisms to ensure officers and staff absent from the workplace can access corporate communications.
- Ongoing concerns regarding recent incidents and lessons learned after separate security breaches in Newtownards and Dundonald, and the perceived lack of detail provided in respect of a timeline of events following the recent security breach at Steeple.
- Workflow concerns in respect of processes followed as part of data extraction and manipulation prior to the breach, including user access and password protocols.
- The need for an independent end to end review of systems, processes and policies.
- Plans in place to risk assess and provide assurance measures for officers and staff.

The Chair thanked the Chief Constable, Assistant Chief Constable Chris Todd, Assistant Chief Constable Bobby Singleton, Assistant Chief Officer Aldrina Magwood, and Chief Superintendent Stephen Wright for their private briefing to the Board.

After PSNI left the meeting Members discussed a number of other matters in respect of this critical incident including the importance of the data breach remaining on the Board agenda for the foreseeable future to ensure regular updates are received, agreed actions are reviewed, and Members can raise queries and concerns; a robust and approved review process is in place to

interrogate all aspects of the data breach; PSNI accountability structures are clearly defined including areas of responsibility; recognition that the data breach is a HR issue alongside the potential ramifications for police operations; recognition that PSNI have provided the Board with solutions and a plan of action going forward; the need for further work to scope a jointly commissioned but independent review process; and the presentation of the Cultural Audit findings to a future Board meeting.

## 4. COMMUNICATION ISSUES

None raised.

## 5. ANY OTHER BUSINESS

None.

The private meeting closed at 1.30pm.

*This was followed by a public media session at 2.15pm in the shared conference room in James House with the Chief Constable and ACC Chris Todd.*

**Strategic Planning & Governance**
**Date:** August 2023

**Chair**