"Protecting From Within"

A review commissioned by the Police Service of Northern Ireland (PSNI) and the Northern Ireland Policing Board (NIPB), into the PSNI data breach of 8th August 2023

T/Commissioner Pete O'Doherty
Senior Responsible Owner

Claire Vickers-Pearson
Lead Author

Foreword

Senior Responsible Owner; T/Commissioner Pete O'Doherty, City of London Police.

"*Every contact leaves a trace*", a well-known phrase attributed to Edmond Locard, a pioneer in forensic science in the early 20th Century. Now over a hundred years on, this notion can be applied within a policing context where every contact, whether internal or external to the police force organisation, leaves a record, or "trace", of data and information. Whether it be the first contact with a victim of a crime where a statement is taken, a crime investigation where a strategy is implemented by a Senior Investigating Officer or a published communications campaign aimed at protecting people from online scams, every service provided by the police, and every decision it makes and action it takes, leaves a digital footprint, a trace of data and information.

The volume of data managed, processed, and stored by policing is vast and continues to increase, both in terms of volume and complexity. Furthermore, policing holds the most sensitive of data and information, and includes personal information about victims, police officers and staff, criminals and police tactics and methodologies. Because of this, data held by policing has the highest trade value on the dark web and we are therefore vulnerable to attacks by external threat actors, particularly those involved in organised crime, or those attributed to hostile states who seek the disruption of the UK economy by destabilising and disrupting critical services like policing.

There are statutory guidelines (for example GDPR) and frameworks (for example ISO 27001) that set out how police forces must control, protect, and use data, but as technology advances and the use of the internet continues to characterise our day-to-day interactions of modern life, the application of this law, policy and guidance into day-to-day policing has become challenging and tricky to navigate.

On the 8th August 2023, the personal information (surnames, initials, ranks/grades, locations, and departments) of 9,483 police officers and staff working at the Police Service of Northern Ireland was published on a public website following a Freedom of Information request. This is considered to have been the most significant data breach that has ever occurred in the history of UK policing, not only because of the nature and volume of compromised data, but because of the political history and

context that sets the backdrop of contemporary policing in Northern Ireland and therefore the actual, or perceived, threats towards officers, staff, and communities.

With the significant threats facing policing by external cyber threat actors, we can't allow ourselves to be vulnerable from within and must do everything in our power to protect our data, information, and infrastructure, and give our staff and members of the public, the absolute confidence and trust that we will protect their information.

In order to achieve this, we must foster a more modern and robust approach to information management and security, and ensure we have the leadership, governance, structures, and systems in place to protect the institution of policing and everyone who is part of it and affected by it. This report not only services to highlight how the breach occurred and what measures must be taken to prevent this from ever happening again, it is a wakeup call for every force across the UK to take the protection and security of data and information as seriously as possible and in this way, many of the recommendations in this report may apply to many other police forces.

This review was commissioned by both the Police Service of Northern Ireland, and the Northern Ireland Policing Board, and I wish to express my thanks to both for so warmly welcoming and supporting myself and the review team during this period. I also to want to express my thanks to each member of the review team, and also the National Police Chief's Council, Police Digital Service, West Yorkshire Police and the City of London Police who have provided the resources that helped to undertake this review.

Pete O 'Doherty

Pete O'Doherty

T/Commissioner City of London Police

NPCC Lead for Information Assurance and Cyber Security

Contents

Executive Summary	Pages 5 - 12
The Context	Pages 13-14
The Incident	Pages 15-17
The Impact	Pages 18-20
Review Findings and Section Recommendations	
Organisational, Governance and Accountability	Pages 21-27
Taking Responsibility	Pages 28-35
Building the Foundations	Pages 36-43
Data Sharing and Usage	Pages 44-46
Data Culture, Talent, and Skills	Pages 47-52
Appendices	
Appendix A: Terms of Reference	Pages 54-60
Appendix B: Methodology	Pages 61-63
Appendix C: Review Team Profile	Pages 64-65
Appendix D: Glossary	Pages 66-67

1.0 Executive Summary

1.1 The Police Service of Northern Ireland (PSNI) is the third largest police service in the United Kingdom (UK) in terms of officer numbers, and the second largest in terms of geographic area of policing responsibility. Following the establishment of the Patten Commission, the Royal Ulster Constabulary George Cross (RUC GC) transitioned to the PSNI on the 4th November 2001. All major political parties now support the PSNI, and form part of the Northern Ireland Policing Board (NIPB) that holds the PSNI to account for the delivery of an efficient, effective, and representative service.

1.2 In a society characterised by the use of technology and data, the PSNI like every police force across the UK, processes and uses a vast amount of highly sensitive data in the day-to-day delivery of its policing services, for example data relating to reports of crime made by members of the public, data on those employed by the PSNI and data held relating to partner agencies the organisation routinely works with. Every organisation that uses, stores, processes, manages, and controls data has a ubiquitous responsibility to protect and safeguard this data, and to ensure that all necessary controls are in place to do so.

1.3 On the 8th August 2023, in response to a Freedom of Information (FOI) request, the PSNI published the personal information of 9,483 police officers and staff on the website *Whatdotheyknow.com.* This breach had a significant impact on the PSNI, the NIPB, officers and staff within PSNI, and wider members of the public. As a result, the PSNI and NIPB jointly commissioned an independent review of the data breach. This reflected a desire to improve, to minimise the risk of any like incident from ever occurring again, and to restore public confidence in policing.

1.4 The independent review is one part of the response to the incident and demonstrates a strong and transparent commitment to learning the lessons. The terms of reference go beyond mitigation and seek recommendations on improvement in the ways data and information are managed to underpin a modern police service in a changing world that is in the midst of a data and technology revolution. The terms of reference are clear that the role of the review is not to apportion blame. Nor is it the role of the review to examine or conduct the organisational response to the breach, which is the focus of the PSNI's Operation Sanukite. The Information Commissioner's Office (ICO) as regulator is investigating the breach including legal compliance, and the review team has been careful not to stray in to this remit, although considers the PSNI should be alive to the possibility of a significant monetary penalty.

1.5 It is now evident, that the breach that occurred was not a result of a single isolated decision, act, or incident by any one person, team, or department. It was a consequence of many factors, and fundamentally a result of PSNI as an organisation not seizing opportunities to better and more proactively secure and protect its data, to identify and prevent risk earlier on, or to do so in an agile and modern way. At the time of the incident, these factors had not been identified by audit, risk management or scrutiny mechanisms internal or external to PSNI.

1.6 This failure to recognise data as both a corporate asset and liability, coupled with a siloed approach to information management functions have been strong contributory factors to the breach. There is little importance granted to essential organisational data functions and they are delivered using a 'light touch' approach. Information and Data Governance are largely absent from organisational strategies, reporting processes and accountability structures, as well as risk registers. Whilst included in the audit programme, this process failed to identify risks and a lack of effective controls. This is no doubt due in part, to the scale of the organisation, its operations and threat landscape. It is also likely to have some considerable basis in the leadership of, culture and attitude towards, these important areas of business that are often seen as complex, niche and best left to the experts. **Data and security are everyone's business and need to be managed and nurtured in the same way as people and financial resources.**

1.7 The need to better prioritise data, information, and cyber security, is not recognised at a strategic level or adequately driven by executive leaders. There is no force programme or strategy. Information Asset Owners (IAO's) are inconsistent. As such, there is an insufficient response at tactical and operational levels. This is despite the passion and drive of some dedicated individuals and teams, and a clear desire to do things right, and "to do the right thing". Structures are outdated, siloed, and require better coordination with resource allocation to these areas of business not reflecting their importance. It is no surprise therefore that associated policies, processes, practices, training, and attitudes, where they do exist, are not effectively adapted and remain too generic. There is an apparent presumption of knowledge in relation to generic Microsoft technologies, and a lower level of understanding of the risk of internal data sharing and good practice. The FOI process has no single comprehensive standard operating procedure, case tracking system or clearly defined roles and responsibilities. PSNI is unique in high levels of usage of FOI by its own officers and staff. The Data Protection Act 2018 is still not fully

embedded, in particular the accountability principles, and there needs to be an improved understanding of what data is processed, more focus on high risk activities and improved monitoring.

1.8 The PSNI is not alone, not within policing, nor across the public sector and further afield yet progress is slow here. This business area is relatively new, fast paced, and complicated. It can also be exciting, and ripe with opportunity. It is most certainly impossible to ignore and requiring of investment. Forces across the UK are at different stages on this journey, and national efforts to aid forces are gathering momentum, offering real support across the service.

1.9 The PSNI has reasonable external and system security protection, although the HR system and associated processes require further attention due to its organic development. It needs to modernise and embed the highest standards of data security, management and governance. Potential improvements could be made in Data Loss Prevention, (Removed for Security Reasons) and the use of the Government Classification Scheme (GSC) application. Challenges to the security of individuals and data itself in the data age are different in modern day policing, not just in Northern Ireland. The Northern Ireland context undoubtedly adds further risk and impetus. The trust and confidence of officers, staff and public at the dawn of the use of new tools technology and techniques are paramount. PSNI and the wider policing community need to respond quickly and learn from this incident. There needs to be genuine commitment to put in place effective governance and controls around all information in order to protect individuals and build trust and confidence in the communities being served. Failure to do so will also result in missed opportunities to improve compliance, reduce risk, and improve reputation and trust. Beyond this, good data management will enable more efficient and effective policing.

1.10 The following recommendations are intended to support PSNI to achieve this, and to minimise the risk of any such data breach happening again. They are based on findings throughout the review combined with the review team's vast awareness and understanding of data and security throughout policing, and specialist and expert knowledge and experience beyond. Many will be of relevance to other police forces, and Chief Constables are encouraged to ask themselves the question of how safe, and how well prepared their forces are.

1.11 Summary of Recommendations

1.11.1 Organisational, Governance and Accountability

-R1. Consider the development of regular rather than exceptional KPIs and reporting regime between PSNI and NIPB, and to the highest level of PSNI.

-R2. Record Strategic risks in relation to Cyber and data value maximisation and compliance, including use in innovative technologies.

-R3. Ensure regular audits of data functions take place, considering co-operation with other specialists within policing or the public sector.

-R4. The role of SIRO (Senior Information Risk Owner) should be repositioned at DCC level, recognising the enterprise nature of the role, and to ensure suitable visibility, oversight, and resourcing.

-R5. The SIRO should establish a Force level Data Board, including clear terms of reference and attendance by Information Asset Owners (IAOs) as well as data business area leads, and other business areas such as digital and corporate change.

- The Board should consider commissioning a data maturity assessment with a view to establishing a data strategy and associated programme of work.
- The Programme of Work should consider the requirement for new capabilities e.g., data governance and data ethics, alongside development of existing services, and coordinate interdependent business areas, such as data management, innovation, and analytical functions.

-R6. Review the SIRO risk registers to capture risks relating to force data assets incorporating all subsets of data and information risk. This should be reported into the Data Board chaired by the SIRO.

-R7. Review the role of SIRO and Information Asset Owners ensuring they are allocated, trained, and supported, and are empowered to manage their information including access to it. Review IAO reporting to ensure coverage across all areas of data risk including sharing, data quality and data protection risk.

-R8. Consider if Operational Support Department is the 'best fit' for the functions of Information Security Unit (ISU), data protection and Corporate Information Branch.

-R9. Consider introduction of a specialist role akin to Chief Data Officer to oversee and coordinate data functions.

-R10. Review the Role of the DPO giving careful consideration to statutory requirements, reporting lines, adequate resourcing. accountability functions, and risk management. The structures and relationships with the ISU, Records Management, Data Protection and Corporate Information Branch business areas should be reviewed.

1.11.2 Taking Responsibility

-R11. Document the FOI process in one Standard Operating Procedure, streamlining and de-duplicating all associated documentation. Ensure the use of flat file formats and safe data anonymisation/review for hidden data are comprehensively covered. Re-design templates and guidance to ensure they are 'user-friendly'. Include version control and how to incorporate and communicate changes to it. Consider a technological solution, such as a case or workflow management system.

-R12. Ensure all involved in the FOI process have clear, documented roles and responsibilities, and there is clarity in relation to who has responsibility for data sign off, what that means specifically and what should and should not be provided to the central team. The publications scheme should be routinely checked. Consider the introduction of specialised local FOI 'Single Points of Contact' supported by regular workshops.

-R13. Strengthen opportunities to enhance the trust with officers, staff, and the public through proactive publication of popular FOI topics, starting with Promotions, Transfers and Temporary postings.

-R14. Build and resource data protection capabilities to meet the requirements of current and upcoming legislation. Consider the need for a force wide information audit, setting up a Register of Processing Activity, and a means to effectively understand and report on corporate compliance. Proactive processes relating to Data Protection Impact Assessments and Information Sharing agreements (ISAs) should be included.

-R15. Review the information assurance process to make sure it is in line with current National Police Chief's Council (NPCC) assurance policies.

-R16. Continue to build cyber defences through the Security Assessment for Policing ('SyAP') and associated security activities.

-R17. Review, streamline, and de-duplicate documentation including service instructions, standards, and policies to ensure they are up to date and in line with the latest NPCC policies, are user-friendly and easily accessible to all who require them.

-R18. Conduct an urgent review of the current GSC policies and application throughout force, including focus on 'SAP' reports, ensuring understanding of the need to classify individual documents, and use effective handling conditions. This should include identification of all PSNI Assets of Official Sensitive or above.

-R19. Determine the on-going need for associated audit mechanism. Ensure the identification, classification, and management (handling, storage, network configuration etc) of force information assets is based on associated risks and value, and consistently applied across the organisation.

1.11.3 Building the Foundations

-R20. PSNI should commence the process to identify the replacement or upgrade options for 'SAP' , ensuring that the selected product is both appropriate for the organisation but can also be supported through its lifecycle.

-R21. Conduct a risk assessment of the role of 'SAP' in relation to Active Directory.

-R22. (Removed for Security Reasons).

-R23. System controls should be strengthened in relation to the 'SAP', and other systems holding personnel data or sensitive operational information. This should include annual resigning of user agreement, review and update of user instructions and policies (including the email policy and alignment to NPCC Cyber policy), documentation, and capture of tacit knowledge to identify and remove any single points of failure. Consider application of security classification, role-based access control, reports only being downloadable to one system location, minimisation of copies, the application of naming conventions, and regular, robust 'review, retention, and disposal' regimes. Consider the requirement for increased audit and monitoring.

-R24. Consider the replacement of current Data Loss Prevention software to cover content not just selected metadata / headline classification.

-R25. Participation in the NPCC Digital Data and Technology Coordination Committee delivery boards and associated activities would provide professional support and learning.

-R.26. The PSNI data warehouse should be expanded to incorporate more datasets, have more use cases and users.

-R27. A Data Maturity assessment should be conducted with urgency to understand the organisational position and develop a programme of work, continuously improving and coordinating existing services and building new capabilities including data governance and data ethics. Stakeholders should include information security, records management, data protection, data management, data innovation and data analysts, alongside staff representative of the broader organisation (for example those in operational or corporate roles).

-R28. Work should begin to identify data domains and high risk/high value data sets, and ensuring data owners, clearly defining the responsibilities and relationship with Information Asset Owners. Consider a proactive, corporate 'Data Quality' and 'Review, Retention and Disposal' programme, prioritising the high risk/high value data assets.

1.11.4 Data Sharing and Usage

-R29. Specific policies and guidance should be produced for all whose roles include the downloading and extraction of data, and its sharing both internally and externally to PSNI. This should cover how to safely download and extract data, and include the principles of data minimisation, classification and anonymisation in line with the relevant ICO Codes of Practice. Consider the creation of a 'Knowledge Repository.'

-R30. The use of the data warehouse should be explored for both internal and external data sharing and queries.

-R31. The ICO recommendations should be progressed (Data Sharing/ Governance and Accountability)

1.11.5 Data Culture, Skills, and Talent

-R32. Explore the possibility of non-generic recruitment and promotion within the FOI area and the areas of information management and security, recognising the specialist nature of the roles and requirement to build experience and expertise as a means of creating resilience across the organisation and high performing teams.

-R33. Consider the identification of data roles and responsibilities on bespoke role profiles and associated regular objectives and development reviews.

-R34. The PSNI college should work closely with the relevant teams to conduct a Learning and Training Needs Analysis across the organisation, including specialist data roles, with a view to then developing an adapted, targeted set of learning products. Due to the heavy reliance on Microsoft Excel, this should form part of the analysis.

-R35. Following the Learning Needs Analysis, a differentiated and role-based bespoke force-wide Data Literacy Programme should be developed, identifying the role of the college and stakeholder departments. Consideration should be given to where data and information disciplines can be included in existing programmes as a golden thread e.g., leadership courses, IT courses, and what bespoke products should be developed and delivered in priority order. Consider the establishment of 'Communities of practice' and 'champion' networks across force.

-R36. Comprehensive, accurate and detailed training records should be held and managed at a corporate level.

-R37. There should be visible executive level support for transparency, information security, risk management, and associated business areas. Consider an executive level sponsored organisational awareness campaign including explaining the value of FOI, the message that information security and management is everyone's job, and of the importance whilst on and off duty.

2.0 The Context

2.1 The data breach that occurred on 8th August took place in a context that served only to exacerbate the impact.

2.2 FOI legislation exists in many advanced countries in some guise and, despite some infamous criticism, remains with us as a fundamental mechanism to increase transparency, enable communities to be further involved in the democratic process, and hold public authorities to account. It allows anyone, anywhere to request written information held subject to certain exemptions, for example where disclosure of the information may adversely impact data protection rights, law enforcement, criminal investigations, and national security. Thousands actively exercise this right, and it has no doubt impacted positively on scrutiny and good, lawful, and ethical governance.

2.3 In a world with rapidly evolving technologies, analytical techniques, and artificial intelligence, alongside increasing data volumes, velocity and variety, private companies and public authorities have struggled to manage the challenge of keeping people and their data safe. Yahoo, Twitter, British Airways, Marriott, Uber, Sony Playstation, Dixon's Carphone Warehouse have all taken advantage of these technologies and suffered subsequent data breaches and GDPR failures. The list is long and growing. Within the public sector, the nature of the information is such that the impact is beyond financial and risks the provision of public services and revealing the information people hold most sensitive. Those to have suffered serious, publicly known data incidents include the Electoral Commission, NHS Wannacry, Barts Health NHS trust, Southend–on-Sea City Council. Policing handles some of the most sensitive data in society in relation to the most vulnerable: officers, staff, victims, witnesses, suspects, and those providing intelligence and information, sometimes at great personal risk. This year has seen a high number of security incidents and data breaches policing in addition to the PSNI data breach subject of this report and two further publicised breaches in Newtownabbey and on the M2 motorway; Norfolk and Suffolk Constabulary revealed vulnerable victim details through an FOI response, Cumbria Police uploaded pay and allowance data to its website, the Metropolitan Police and Greater Manchester Police suffered data breaches following cyber-attacks on their supply chain involving officer details, and many more.

2.4 Adding to this, it is difficult if not impossible in 2023 to preserve anonymity whilst fully participating in society as our lives are lived online. Personal data is an extension of oneself,

and this cannot be kept safe behind closed doors. We have to share our personal data to access essential services quickly and easily, to both buy staples of modern life at a favourable price and for the convenience needed to meet the challenges of busy lives, to keep in touch with our nearest and dearest who may no longer live down the road in modern society, and for wellbeing and enjoyment in hectic lives pursuing hobbies and learning about what is important to us. Keeping track of what has been shared with whom is difficult enough, without numerous passwords, social engineering, data brokers, and online criminals to navigate.

2.5 Much about Northern Ireland is unique, including its political and policing context. 'The troubles' in Northern Ireland are well known and well documented, as is the 'Good Friday Agreement', and since 1998 society has enjoyed relatively peaceful times. The relationship between the public and the police is so fundamental to peace that the Report of the Independent Commission on Policing in Northern Ireland dealt specifically with this and set out a blueprint for the future to improve relations and maintain security. The current threat level is set at 'SEVERE'. Many spoken to as part of our review told of the recent destabilisation within Northern Ireland Society due to economic challenges, the suspension of the Northern Ireland Assembly, political uncertainty, controversy in relation to senior decision making within PSNI, and pertinently the recent and shocking shooting of DCI John Caldwell. This cannot be ignored in understanding the impact of the data breach.

2.6 The data breach cannot be undone. Questioning whether it could have been avoided cannot reverse what has happened. To understand what can reasonably be done to reduce the risk of it happening again, minimise the impact if it does, help people to move forward and restore trust, the review seeks to identify the causes on a micro and macro level and offer recommendations for the PSNI. Alongside the broader response to the incident under Operation Sanukite, opening itself up to independent scrutiny is a positive step.

2.7 The data breach must not be seen as an opportunity to undo progress. It is an alert to ensure the protection of officers, staff and the public, and their data, is fit for purpose in the context of 2023 and beyond. Officers and staff can then continue with their work, taking advantage of the latest tools, technologies, and techniques to make Northern Ireland safe for all.

3.0 The Incident

3.1 The following timeline sets out the steps taken to process the request that led to the data being breached from receipt to response.

3.2 3rd August

- FOI request received within Corporate Information Branch via 'What Do They Know' website in the name of (Removed for Data Protection purposes). The request asks for the '*number of officers at each rank and number of staff at each grade in tables as of 01/08/2023'.*
- Six minutes later, FOI request received within Corporate Information Branch via 'What Do They Know' website in the name of (Removed for Data Protection purposes). The request asks for the '*number of officers at each rank and number of staff at each grade distinguishing between how many are substantive/temporary/acting as of 01/08/2023. Could you please provide this information in the form of tables for officers and tables for staff'.*
- The requests are aggregated for cost purposes in line with FOI legislation, logged locally as FOI- 2023_02505 and an acknowledgement is sent to the requester by CIB (Person 1).
- Strategic Communications and Engagement Department are advised of what FOIs have been received in line with normal protocols and identify this one as being of potential interest to them in terms of potential media interest.

3.3 4th August

- Request is assessed by CIB (Person 2) to relate to a single business area and sends it to HR (Person 3) .
- HR (Person 3) sends request on HR (Person 4) with deadline of 8th August, with case tracker document for completion. HR (Person 3) logs the request locally.
- HR (Person 4) From an existing report (Combined '3c' and 'Per List'. These are individual HR reports) and HR System ('SAP') download, they create a pivot table, then a further tab for the response.

3.4 7th August

- HR (Person 4) saves work as a master file.
- HR (Person 5) is tasked by HR (Person 4) to prepare the document for release.
- HR (Person 5) checks the formatting, that the response matched the question,

there were no formulae present, and there was no high-risk information. They remove all visible tabs, which required a move of the tab bar to the right, obscuring the first tab but for three dots indicating a hidden tab.

- After being called away for another work-related matter, five to ten minutes later HR (Person 5) returns to the FOI request. They delete the visible tabs, with only the response tab then visible on screen. They are unaware of the meaning of the three dots and did not remember there was a tab to be removed on the left. This was the 'SAP' download tab. HR (Person 5) closes the spreadsheet and returns it via email to HR (Person 3) with the completed case tracker.

3.5 8th August

- HR (Person 3) sends the email and spreadsheet to HR (Person 6) for quality assurance, advising of the due date of 9th August i.e., 1 day later.
- HR (Person 6) reviews the spreadsheet response tab, unaware of the hidden tab identified by the three dots and returns it to the HR (Person 3) via email with approval.
- HR (Person 3) sends the email including case tracker and spreadsheet attachment to FOI, updates the local log, and stored the correspondence for audit purposes.
- The response is received within FOI and checked for completion and identified as a full response with no identified harm by CIB (Person 2) , who then save the trail locally for audit trail purposes. They then allocate it for response to CIB (Person 7).
- CIB (Person 7) checks the case tracker again to ensure there is no harm. They copy the spreadsheet and rename it, also removing details of the extracting department and system that were recorded in it. They attempt to copy the response from the spreadsheet to the letter response template and is unable to due to embedded formatting in the letter template. They 'tidy up' the spreadsheet copy, changing font and colours. They upload it to the local case management system. They send Strategic Engagement and Communications (Person 8) a copy and is advised there are no issues.
- At 14:32, CIB (Person 7) issues the response with covering letter and spreadsheet to the responder on the

'What do they know' website. They complete the internal checklist and send a copy to the Executive Support team.

3.6 It is discovered later the same day that the spreadsheet in fact includes a further tab of the original 'SAP' download containing 32 columns including the surname, initials, rank/grade, role, service number, department, location, duty type and gender of all serving officers and staff (9,483). This has been published on the internet and remained in the public domain for almost two and a half hours.

4.0 The Impact

4.1 The right to privacy is a human right and the Data Protection Act 2018 also safeguards this right. Personal data in the public domain can be harmful. In addition, the more information there is, this builds and increases the chances of identification with potentially harmful and even catastrophic consequences. When this is combined with other publicly available data, for example what can be found online or what is known by others, it makes identification of an individual even easier. In the age of the internet of things, it is difficult to keep track of personal information that is out there, and even more difficult to control it.

4.2 For any one individual, the more information publicly available, the higher the risk of identity theft or financial crime. For those working in policing, it can open up potential abuse from sections of society who do not respect the service. For those in specific roles, such as undercover or covert roles where officers and staff work in close proximity to criminality, the risk of harm from identification increases. For PSNI when this is combined with the community tensions and attitudes of some towards the police and reform, the potential for harm is high, this is compounded further.

4.3 It is quite normal for officers and staff in sensitive roles across the police service, for example those working with Organised Crime Groups or involved in Counter Terrorist Policing, to keep their roles private, and even for those working within the service to avoid disclosing who they work for to acquaintances. Outside of Northern Ireland, it is less usual for this to be kept from friends and even close family for fear and avoidance of repercussions to individuals, and to their families and friends. This is the reality for many PSNI officers and staff. Whilst officers and staff may take additional personal security precautions and have protective measures in place, they are also members of the community with no additional rights or means of self-protection than the rest of us. Staff associations reported already low morale and disengagement from senior ranks amongst their members.

4.4 A surname can help to identify a community background, religion or ethnicity. There are many families who have multiple serving family members. A rank, grade or department might indicate potential involvement in certain cases or activities, and a work location would assist in finding someone.

4.5 The 'Terms of Reference' describe the damage caused by the data loss as

'unquantifiable' to the confidence of officers, staff, partners, and the public. Whilst it cannot be quantified, and it is difficult for those not directly involved to understand, it can be described to some extent, and also felt when listening to those impacted.

4.6 The review team encountered a vast range of responses from officers and staff, ranging from ambivalence, to concern to palpable fear. People also expressed distress, sadness, and dismay. Many expressed and displayed a strong resolve to continue serving the communities of Northern Ireland and keeping them safe.

4.7 Of the 9,483 people involved, over 4000 proactively contacted the threat assessment group set up by PSNI as a means of support and information. A similar number are thought to be part of a complaint to the ICO, and a civil action against the force. At the time of the review, it was reported that no one had been moved for their safety, although one officer felt it necessary to relocate to keep themselves and their family safe. Some have temporarily relocated as the situation progresses and until they feel in a position of safety. The Staff Associations advised the review that there were some who would like to but without the financial means to do so, most particularly junior and younger personnel. Those with less service are experiencing real concern for the first time in their service due to recent events. One resignation has been received citing the impact, and over 50 reported sickness absence linked to the data breach at the time of the review visit to PSNI. Officer and staff mental health in particular has worsened, and there are additional pressures on welfare services and line management. It has been reported that many have been unable to access public wellbeing and mental health support services in a timely manner when needed and cannot afford access to private health services. It was reported that officers and staff had asked if they could be supported in name changes previously and advised this was unnecessary. The review team heard of officers and staff now too frightened to visit friends or family, who have withdrawn from the social aspects of the lives, and who fear visiting their place of worship. Staff association membership has increased significantly as a direct result of the data breach, as has the number and frequency of contacts. Lack of clarity in relation to the threat assessment status is cited as having worsened the situation as it was not clearly understood that this did not relate to the actual threat to an individual, but how quickly it was necessary to speak to them in order to conduct an effective threat assessment.

4.8 Beyond the personal impact, Assistant Chief Constable Chris Todd reported to a parliamentary select committee that the financial impact could run to between 24 to 37 million pounds, a sum that any police force could ill afford, and at a time when financial constraints for the PSNI are already beginning to have consequences. This figure includes home security elements, litigation, and a potential regulatory monetary penalty.

4.9 The potential for operational consequences for the force is high. With recruitment and retention already problematic, especially amongst certain communities, this incident is unlikely to provide confidence to those wanting to become part of the service but fearing identification. There is a risk to the free flow of intelligence, the lifeblood of policing, if those providing it cannot be reassured that they can do this in confidence. Staff associations also articulated that even those amongst them who have thus far felt reasonably comfortable standing up for progress and their beliefs now feel less so. Of particular concern is the lasting impact and potential for future exploitation of the information if the page is turned too quickly, or lessons are not taken seriously or change fully embedded.

4.10 Whilst examining the effectiveness of PSNI's response to the incident is outside the scope of the terms of reference, it is fair to acknowledge the organisation's swift action to provide reassurance through additional patrols, additional security measures for some officers deemed to be at higher risk, the threat assessment line open to all officers and staff, rapid arrests, and prosecutions of those found to have the information. The support provided to individuals by the staff associations should also be acknowledged. It is hoped that the findings of this review and their implementation will assist to restore confidence and build reassurance and security beyond previous levels.

5.0 Organisational, Governance and Accountability

5.1 It is generally recognised that within an organisation, culture and change are driven by visible and decisive senior behaviours and focus starting from the very top.

5.2 Amongst the responsibilities of the NIPB since the Patten review, and in line with the Northern Ireland Justice Act 2000, is to hold the Chief Constable of PSNI to account for the delivery of services. Its states that one of its objectives is to "*To monitor, oversee and assess the performance of the PSNI through the Board and its Committees and to ensure the delivery of Human Rights based, community focused policing*." As there were no associated key performance indicators in place between PSNI and the NIPB in respect of this area of business, and PSNI audit and risk mechanics had not picked up any issues, the subject of data and information handling has not appeared on NIPB committee agendas.

5.3 The consideration of data as a corporate asset with associated high-risk liabilities when developing future NIPB Corporate and Business Plan objectives would be beneficial in increasing the accountability and scrutiny of PSNI in this respect. The PSNI Digital and Transformational Change Strategies identify the need to be evidence based, and harness technology, although there is no clear plan of how to do this whilst also keeping the data secure.

5.4 Another opportunity to have data on the radar would be a public satisfaction measurement in a satisfaction survey or similar relating to transparency, privacy, or trust in how data is handled. It is recognised that the options of what to measure are extensive, and focus must be given to what are considered the most meaningful measures.

5.5 The same reasons would account for a lack of visibility at Chief Constable level. Both risk and audit processes appear structured and robust, feeding into the Strategic Management Board chaired by the Chief Constable. This might indicate a positive picture, but on further examination this unfortunately does not appear to be the case. The Annual Governance Statement 2022-23 has good coverage of information security and technical controls yet is more limited in terms of data protection. This is also mirrored in the reporting to the Audit and Risk Assurance Committee (ARAC), with the main omission relation to the accountability requirements of the Data Protection Act 2018. Neither information security, data protection nor data governance security appear on the corporate risk register. The recent ICO audit found limited assurance in relation to data

protection (Governance and Accountability), and Information Sharing, suggesting a lack of effective oversight to this area of business.

5.6 It is positive to see that a Cyber risk has since the time of the review been considered for addition to the strategic risk register. Organisations will have this as part of their scanning given the rapidly changing nature of the cyber threat, and the potential impact. However, it must be understood that this relates to the organisation's technical ability to protect itself from outside threats. Risks in relation to internal threats, non-compliance, and lack of safe lawful and ethical use of data are distinctly different, and should not be overlooked, ensuring protection from the inside. The PSNI's performance on the newly implemented national annual cyber Security Assessment for Policing (SyAP) that measures how cyber secure a police force is, has been reasonable but there is significant room for improvement. The 'reasonable' rating is when compared to the desired level of maturity overall. This is a holistic security assessment covering technology, physical, people and processes based on the principles of the National Institute of Standards and Technology (NIST).

5.7 The SIRO risk register is diluted to two levels below the Strategic Management Board and Organisational Risk Register. In a mature organisation there may be no need for a separate information risk register as the understanding of risk associated to data assets would be understood in the same manner as finance or people. To find this is rare as there is generally a much lower level of understanding of the identification and mitigation of information risk. The data discipline is relatively new in comparison. It is overseen by the SIRO at Information Governance Delivery Board (IGDG) chaired by the SIRO (Assistant Chief Constable Operations Support) and then reported through the Strategic Performance Board chaired by the Deputy Chief Constable by exception, and then to the Strategic Management Board also by exception.

5.8 In addition, the PSNI SIRO risk register does not cover organisational information risk and resembles closer a local departmental risk register for the information compliance business area, rather than across the service. In addition, there is a further risk register held within the ISU reported in through Information Governance Delivery Group (IGDG). This is a requirement of the National Policing Community Security Policy, National Policing Community Security Principles, National Police Information Security Risk Management Framework, and the National Police Information Security Risk Assessment Guidance. It covers personnel, physical, procedural, and technical risks relating to

information security across the organisation. There is no risk register capturing broader categories of information and data risks including compliance with primary legislation, privacy risk, unlawful processing, poor data quality, and excessive processing. The role of IAO seems similarly limited and poorly understood, as is the case across many organisations and police forces.

5.9 The role of SIRO sits at Assistant Chief Constable level, and in the reporting line of the business areas delivering services to identify and mitigate information risk with a potential impact on 'proximity blindness.' This positioning of the SIRO role is out of kilter with most policing organisations where it sits at DCC level along with other corporate risk given that a DCC has a complete end-to-end view of all aspects of the organisation. Having the DCC as the SIRO also reflects the importance and priority the organisation places on information management and security. It is possible that the SIRO role sits here organisationally due to a misunderstanding of a legal position stating that the ACC Organisational Support can sign off the use of the section 36 exemption in response to FOI requests where disclosure might prejudice the effective conduct of public affairs.

5.10 Numerous audits have been scheduled across the areas of information security, data protection and FOI, although some have been delayed or cancelled. Of the ones conducted, assurance levels have been reported as adequate. The scope of these audits has however been limited in their coverage. They have entailed system accreditation, data breaches, Data Protection Impact Assessments (DPIAs), specific GDPR requirements and FOI compliance (although the FOI audit did have data protection in the title but not in the report). In June 2019, an internal audit on the implementation of GDPR returned a 'satisfactory rating' subject to the completion of stated actions within 12 months. Whilst some of these actions remain outstanding today, the review team found no evidence of a re-audit, or escalation of the matters beyond IGDG. Security incident data is reported to the Audit Committee on a quarterly basis.

5.11 The audits have also had limited focus on the existence of service instructions and process documentation, yet no reality testing of application or understanding. They have also been conducted by generalist auditors who may lack the required skills or knowledge required to conduct effective audit in such a specialist field. There is no evidence of inter-force or public agency peer review or comparison.

5.12 Whilst the data breach took place as a result of an FOI request, and the report will show

some contributing factors in the way FOI requests are processed by the PSNI, it is more specifically a security incident and a data protection breach. The review has found that PSNI has been slow to adapt to the requirements of new data protection legislation changes. The current Data Protection Act came in to force in May 2018, with an 18-month period prior to this where implementation was encouraged by the ICO and across policing by the National Police Chief's Council. The legislation was enacted with no 'grace period' and this was made clear by the regulator. A Data Protection Act implementation plan presented to IGDG then to the Strategic Performance Board in 2021 shows clearly that implementation is far from complete. Progress had been made since although it could be said that the progress is optimistic or even over-stated. It includes green ratings where the narrative identifies that the required actions are 'to be' completed, and a final position of only providing specialist training or ad hoc information sharing guidance only on request. It remains unclear if the requirements for all processing activities to be recorded along with related information in a register is met some 6 years after the requirements were known. This is a fundamental corner stone to any data protection programme. The report also identifies that obligations in relation to DPIAs are not being met, yet this is recorded as 'green' and information sharing requirements not being met are identified as 'amber'. The upcoming Data Protection and Digital Information Act will bring some changes but overall, the legal obligations will remain similar in a policing environment.

5.13 The 'IGDG' is the PSNI forum for the monitoring of secure and lawful management of data and information, including both personal and operational data. It has clear terms of reference and sits regularly. The terms of reference refer to an annual report to the Chief Constable, although it is not clear if this happens consistently. The terms of reference also refer to 'Cyber and Records Management Strategy' and 'Data Protection Compliance', but no 'Data Protection Strategy', which could be beneficial to PSNI to ensure continuous improvement. The data protection business area was only introduced in 2018, and the other areas are much more embedded in the organisation. It could be beneficial to bring them together under one umbrella as an 'Information Governance' pillar of a broader Data Strategy, as recommended by NPCC on the introduction of the Data Protection Act 2018. This has the benefit of an expert with a 'helicopter view' across an interdependent, technical business area with support. IAOs are not however required to attend the IGDG. Indeed, there is no official forum for IAOs to report on or be held to account on performance. The agenda regularly

covers Information Technology Security, and compliance with Right of Access timescales and complaints, but again little in relation to data protection for accountability requirements, DPIAs, Data Processing Contracts, joint controller agreements, or Information Sharing Agreements (ISAs). A progress report on data protection including survey results and generic ICO audit report recommendations was submitted stating that progress had been made but more was needed, concluding that the "DPO continues to seek more innovative ways to continually promote the data protection agenda and improve understanding and compliance" .

5.14 The Data Protection Officer (DPO) role in PSNI was created in response to the requirement in the Data Protection Act 2018. The progression of the establishment and embedding of the role has unfortunately been impacted by a period with a temporary DPO, and a period where the post was unoccupied (Removed for Data Protection Reasons). The role has no direct reporting mechanism to the most senior level of the organisation, which is a legal requirement.

5.15 There also seems to be a lack of recognition of the breadth of the role, in comparison to a very well-established ISU, resulting in a skewed focus. It is unusual to see records management being discharged alongside information security function with data protection and access to information functions including FOI and Subject Access being separated. It is more usual to see them discharged under one function. Often this is overseen by a senior role incorporating the role of the DPO and often Information Security Accreditor. Joint working between the DPO and information security lead was reported to the review. This overarching function appears to be conducted by a senior police officer who also shares these responsibilities with significant operational duties. Given the rapidly evolving nature of this complex business area, expertise, consistency, and stability is key.

5.16 The ICO audit conducted in summer 2023 identified some key areas for improvement, reiterated by the review team. Responses to the ICO recommendations indicates that peer support and networking outside of PSNI with experts from similar organisations to ensure self-awareness would be of benefit. Key recommendations included embedding of Data Protection Risk Assessments (DPIAs) in project methodologies, consideration of 'champions' throughout the force, ISA review, policy application testing, targeted training, and external audit. It is a statutory obligation to conduct a DPIA to identify and manage any potential impact on the rights and freedoms of individuals through high-risk personal data

processing in all cases. Policing employs lots of potentially private intrusive tools and technologies such as Automatic Number Plate Recognition, bulk and sensitive information sharing, facial recognition, internet search tools, and algorithmic risk assessment tools.

5.17 Moving from the defensive to the offensive, it is impossible to fully appreciate the risk associated with data assets without understanding the potential value. Another route to senior visibility is inclusion in strategy. The Digital Strategy makes mention of data. It talks of the aim to be "evidence based" and "informed by the objective consideration of data," and it also talks of building trust, cohesion, and respect of the rule of law through technology. DPIAs are crucial to this. It is however very technology focussed despite technology regularly being the enabler to release the value of the data asset. The two are inextricably linked, and therefore a logical step for a data strategy would be alongside a technology strategy. And the services need to work closely together. Data has a risk/ compliance requirement, but it also has a requirement to be managed and nurtured so it can be used effectively.

5.18 Whilst the review team was able to identify pockets of related activity and good practice across the force, such as the existence of a data warehouse and some data quality activity, there is an absence of strategy, coordination and ownership or drive. There appears to be no understanding of the data maturity, albeit a maturity assessment had been scheduled and was postponed until after this review.

5.19 The Human Rights Advisor to the NIPB produced a report in July 2023. It highlights the correlation and alignment between data protection and article 8 human rights, and the need to transparently ensure compliance with both in order to gain and maintain public support for privacy intrusive tools, techniques, and methodologies. It uses the examples of surveillance, biometrics, facial recognition, mass data sets, digital data extraction. Data ethics, governance and quality are essential for their effective, safe, and lawful deployment. The review team would support the recommendations.

5.20 Section Recommendations

-R1. Consider the development of regular rather than exceptional Key Performance Indicators (KPIs)) and reporting regime between PSNI and NIPB, and to the highest level of PSNI.

-R2. Record Strategic risks in relation to Cyber and data value maximisation and compliance, including use in innovative technologies.

-R3. Ensure regular audits of data functions take place, considering co-operation with other specialists within policing or the public sector.

-R4. The role of SIRO (Senior Information Risk Owner) should be repositioned at DCC level, recognising the enterprise nature of the role, and to ensure suitable visibility, oversight, and resourcing.

-R5. The SIRO should establish a Force level Data Board, including clear terms of reference and attendance by Information Asset Owners (IAOs) as well as data business area leads, and other business areas such as digital and corporate change.

- The Board should consider commissioning a data maturity assessment with a view to establishing a data strategy and associated programme of work.
- The Programme of Work should consider the requirement for new capabilities e.g., data governance and data ethics, alongside development of existing services, and coordinate interdependent business areas, such as data management, innovation, and analytical functions.

-R6. Review the SIRO risk registers to capture risks relating to force data assets incorporating all subsets of data and information risk. This should be reported into the Data Board chaired by the SIRO.

-R7. Review the role of SIRO and Information Asset Owners ensuring they are allocated, trained, and supported, and are empowered to manage their information including access to it. Review IAO reporting to ensure coverage across all areas of data risk including sharing, data quality and data protection risk.

-R8. Consider if Operational Support Department is the 'best fit' for the functions of Information Security Unit (ISU), data protection and Corporate Information Branch.

-R9. Consider introduction of a specialist role akin to Chief Data Officer to oversee and coordinate data functions.

-R10. Review the Role of the DPO giving careful consideration to statutory requirements, reporting lines, adequate resourcing. accountability functions, and risk management. The structures and relationships with the ISU, records management and Corporate

Information Branch business areas should be reviewed.

6.0 Taking Responsibility

6.1 Policing processes large volumes of personal, private and both operationally and commercially sensitive information. There is a complex legal, regulatory and compliance landscape surrounding the use, processing, and management of police information, both from a legislative and service regulation perspective. Northern Ireland has further legal obligations under the Public Records Act and Disposal of Documents Order, which have not formed part of this review.

6.2 Handling personal data with care is important to engender, improve and maintain public trust, and something which is at a premium within our service given the powers entrusted to us in our mission to keep the peace, prevent and disrupt crime, and protect people from harm. As such, more stringent obligations are placed upon the police service and law enforcement partners to follow the UK GDPR and part 3 of the Data Protection Act 2018.

6.3 Transparency and accountability are achieved in part by public authorities, including police forces, through compliance with the Freedom of Information Act 2000. The legislation requires the public authority on receipt of a written request to provide a copy of information held within a time period of 20 working days. This is subject to the application of certain exemptions such as data protection, law enforcement, and prejudice to a criminal investigation or national security, amongst others. Police information and data have the highest trade value on the dark web, and therefore policing is particularly vulnerable to external threat actors such as organised criminals and hostile nation states. This is reflected in the number and range of cyber-attacks that have impacted policing throughout 2023, and includes the attack on the Association of Chief Police Officers Criminal Records Office and Digital ID. The resulting impact of a cyber-attack on a single force and the entire UK police service could be devasting. The risk is so great that policing has a stringent set of requirements and controls set out within the NPCC Assurance Policy and the Security Policy Framework. Maturity is assessed through the 'SyAP'. The Police Digital Service 'Cyber Services' National Management Centre carries out monitoring on behalf of all forces and has identified numerous attacks that have been managed through the NPCC Police Information Assurance Board led gold command structure. There have recently been attacks to the third-party supply chain and criminal justice partners that have been

managed in this way to support forces, also involving the National Crime Agency and National Cyber Security Centre.

6.4 The review team identified both good practice and potential improvements to PSNI services in this area that would assist in reducing the risk of any data breach reoccurrence and mitigating against both their likelihood and impact.

6.5 There is within specialist teams much dedication, a well-established cyber security and physical security culture, and controls. Recent years have seen some hard work and progress across all areas.

6.6 However, teams and departments work largely in siloes, leading to communication gaps and inefficiencies, and there is an apparent feeling of reliance on specialist services. There is also a reliance on generic, self-taught training methods, an excessive amount of policy documentation, and poorly defined processes, and roles and responsibilities. There is scope for improvement.

6.7 Some recommendations for improving data protection performance have been addressed earlier in the report.

6.8 In addition, data protection services are 'light touch,' with heavy reliance on the DPO and Head of Information Security, and limited appreciation and discharge of the responsibilities across force beyond the most basic. There is no clear route for the DPO to have access to bring serious concerns to the attention of the most senior level of the organisation i.e. the Chief Constable, which is a requirement in law. The DPO is involved in providing education and training for the workforce with a generic mandatory e-learning package for everyone. There is an absence of bespoke training that is required to ensure that the appropriate level of confidence, competence and capability exists in the right places across the organisation.

6.9 The DPIA function is developed with very low numbers of DPIAs being conducted, and with a passive process which requires those across the service to come forward when one is required. The approach to compliance is generally relatively passive, relying on extensive service instructions and documents on the PSNI intranet and content management data base 'POINT' unless business areas are self-aware and knowledgeable enough to seek further support. There is little in the way of verification or validation processes, or targeted support based on risk and knowledge of high-risk data sets or processing activities. In addition, the Information Asset Register, which identifies organisational data assets and related information, appears to be relied upon as the

Register of Processing Activity (ROPA). A ROPA is should be the output of an information audit and information flow mapping exercise identifying specific processing activities using personal data, and includes details such as where the data comes from and flows to, what the lawful basis for the specific processing is (for example consent or for a law enforcement purpose) and other information. It is an essential tool in effectively managing personal data, and a legal requirement.

6.10 There is a lack of data protection audit and ability to understand force wide compliance, although the bi -annual survey approach is a positive step. This is limited however by a generic approach and lack of targeting high risk and high interest areas, such as staffing data, data relating to covert activity, intelligence, and suspect, victim, and witness data. There was a poor response rate, below 10%, with obvious risks to relying on this to paint a realistic overall picture. The 2021 survey reported that the DPO stated that there were sufficient resources to deliver the service, albeit some interviewees did not agree with this. The review team has not had sight of any request for resources. A more proportionate distribution of resources across information compliance functions should be a consideration. The areas recount close working relationship which might benefit from review and formalisation, ensuring clarity and lack of duplication.

6.11 There is a risk in all organisations that subject matter experts can become isolated and feel unsupported. Specialists across these areas may benefit from networking with 'critical friends' outside the organisation sharing the same difficulties. This should include more contact with peers from the Criminal Justice Community both within Northern Ireland and beyond with whom there will be more areas of shared understanding.

6.12 Freedom of Information

6.12.1 The FOI unit within the Corporate Information Branch functions well, and more recently, statutory timeliness compliance has been significantly improved and is high compared to other police forces across the UK following a period of monitoring by the regulatory authority. Whilst the data breach resulted from an FOI request, the fundamental issues are not solely related to the organisation's response to FOI requests. Review of all previous published FOI responses over a 2-year period covering thousands of disclosures, demonstrates that the process is largely free of data breaches. The PSNI process does not differ significantly from other forces; resourcing levels are high and have recently been increased.

Whilst the force receives a large number of requests, approximately 20% of these have been identified as being internally generated from serving officers and staff.

6.12.2 The review has identified 4 key areas for improvement:

- Fragmented, inconsistent, and excessive documentation, with lack of clarity and understanding of roles and responsibilities.
- Demand management of internal FOI requests
- Guidance on the extraction, minimisation and anonymisation of data. This will be covered in more detail later in the report.
- Training and awareness. This will be covered in more detail later in the report.

6.12.3 PSNI would benefit from one single, comprehensive FOI Standard Operating Procedure (SOP) that is familiar to all FOI staff and others involved in the process. Their service instructions and e-learning are extensive, and largely duplication between them and with the legislation itself. The detail contained is excessive for the purposes of the vast majority of the force beyond specialists. It might be more effective were it to be less detailed and generic, with procedural detail being contained in the SOP. The process is made up through a mixture of various individual documents such as logging spreadsheets, audit logs, checklist, eLearning, guidance notes, emails and templates. Many organisations use a case management and workflow request tracking system. A number of interviewees described the documentation as not being 'user-friendly.' There is a heavy reliance on tacit knowledge, experience, the local, unstructured sharing of knowledge, and on seniority as a substitute for expertise. There is inconsistency in understanding within the FOI team, such as what would constitute 'creation' of information as opposed to 'Information held.' There is evidence of some dip-sampling, although periodic reviews or audit policies for processes were found to be limited.

6.12.4 The 'SPOC' role in business departments differs to that found in most forces, where this is seen as less of a distribution role, and more of a trained and supported 'gatekeeper' role with specific documented responsibilities, such as checking for hidden data, and support to enhance their expertise. Business area leads recounted ambiguity as to what should be provided to the FOI team; is it all information required to arrive at the response, or is it all information forming the response only? There is no guidance either within the FOI team or business units in relation to safe data extraction,

and no clarity on safe file formats. There was evidence of local 'interpretation' of the request as opposed to seeking clarity.

6.12.5 Whilst there is some proactive publication, and an extensive disclosure log of previous responses, this is limited and apparently not based on any regular analysis of the nature and volumes of requests received. There is some evidence that the disclosure log is reviewed before responding to a new request, although not that it is systematic across the whole team. Whilst some of the information for the request leading to the data breach was already present on the website following a previous request, this would not have made a significant difference to avoiding data breach as the further questions on this particular request would still have needed to be processed. The number of requests relating to promotion, transfer and temporary posting is vast compared to other forces, and thought should be given to how this might be addressed via other means to reduce the burden.

6.13 Information and Cyber Security

6.13.1 Whilst not covered in detail by primary legislation, the importance of information security cannot be overstated. A clear differentiation between protection from external threats, and internal malicious or accidental threats needs to be made, and services delivered proportionately. In some ways, it could be argued that technical controls, whilst complex in their own way, are easier to manage than human factors.

6.13.2 PSNI has reasonable cyber security protection maturity compared to other forces. At the time of the review PSNI was amongst the top three in the country according to the recent 'SyAP' security maturity assessment. Further forces have now completed the assessment and the position has lowered yet is still relatively high in comparison to some forces. IT system accreditation and risk management is good, there are completed system risk assessments for all major system which are kept up to date with technical risks being identified and managed.

6.13.3 PSNI do have a current risk appetite statement, and this ought to be robustly applied to information risk management decisions, alongside consideration of broader operational risk with a documented process. There are potential unintended consequences of risk aversion such as over reliance on internal systems and management, such as the use of out-dated systems, additional cost, and failure to adopt technologies facilitating modern working practices and security features e.g., Office 365, and 'SAP'.

6.13.4 The organisation has recently onboarded onto the 'SyAP'. This is a bespoke assurance set

developed for UK policing. It is based on the NIST Cyber Security Framework, also incorporating the specific security assurance question sets developed for the National Enabling Programme and the Governance and Information Risk Return previously in use by the National Police Information Risk Management Team.

6.13.5 The 'SyAP' is designed to cover the full range of security; physical, personnel, procedural, technical and resilience, and to be a continual assessment and assurance mechanism.

6.13.6 Therefore, a number of controls relevant to information security will be reviewed to ensure that where improvement can be made this is captured. The findings impacted by this report have been incorporated into the recommendations or will be considered as part of 'SyAP' business as usual. They include security classification, roles and responsibilities, threat monitoring and response, risk management processes, training, and access controls. The National Audit Risk and Compliance Team will discuss existing maturity ratings with the PSNI's ISU and recommend appropriate changes.

6.13.7 PSNI have adapted the principles of the Security Policy Framework (albeit an older version) into 2 key documents, Accreditation Processes Good Practice Guide, and the Accreditation for Information and Communication Services (ICS) Project Managers. Both of these documents provide a high level of detail on the process, and require enduring accreditation of PSNI systems through life, and reference the HMG Information Assurance Standards Numbers 1 and 2. There is a requirement to re-accredit system through life at set periods. The Information Assurance Unit maintains an accreditation register which covers a sizeable number of systems operated by PSNI, the vast majority of which have been fully accredited, including those which are within the scope of this review. All targets of accreditation have an assigned IAO and lead accreditor, plus a clearly indicated re-accreditation point.

6.13.8 Whilst the above approach does ensure that mitigations are effective at key points in the system lifecycle, the gaps between formal re-accreditation may not allow for the management of change as well as more flexible assurance processes. The Information Assurance Standards 1 and 2 have been depreciated for several years and current NPCC policy reflects a Secure by Design approach, coupled with through life assurance, which would allow for greater efficacy in the assurance process.

6.13.9 The biggest areas of concern are excessive and generic service instructions and

standards, lesser developed auditing and monitoring controls, and most significantly poor embedding and application of the GSC.

6.13.10 There remains ambiguity around data classification with many still referencing the "CONFIDENTIAL" category, and IL4 standard. Data from 'SAP' is exported to Excel without consistent application of classification or handling instructions. Beyond system level, there appears to be no systematic identification of high risk and high value assets, with an apparent perception that everything is equally sensitive, leading to lack of focus on the most sensitive assets. There is a broad perception that individual documents and assets do not require a classification except when in transit via email. Beyond perception, this was specifically stated by some interviewees. A data classification review is required of all datasets on the corporate network to ensure proper data handling and training provided to all PSNI officers and staff. There should be a process for a classification review for new data products and when they are published.

6.14 Section Recommendations

-R11. Document the FOI process in one Standard Operating Procedure, streamlining and de-duplicating all associated documentation. Ensure the use of flat file formats and safe data anonymisation/review for hidden data are comprehensively covered. Re-design templates and guidance to ensure they are 'user-friendly'. Include version control and how to incorporate and communicate changes to it. Consider a technological solution, such as a case or workflow management system.

-R12. Ensure all involved in the FOI process have clear, documented roles and responsibilities, and there is clarity in relation to who has responsibility for data sign off, what that means specifically and what should and should not be provided to the central team. The publications scheme should be routinely checked. Consider the introduction of specialised local FOI 'Single Points of Contact' supported by regular workshops.

-R13. Strengthen opportunities to enhance the trust with officers, staff, and the public through proactive publication of popular FOI topics, starting with Promotions, Transfers and Temporary postings.

-R14. Build and resource data protection capabilities to meet the requirements of current and upcoming legislation. Consider the need for a force wide information audit, setting up a Register of Processing Activity, and a means to effectively understand and report on corporate

compliance. Proactive processes relating to DPIAs and ISAs should be included.

-R15. Review the information assurance process to make sure it is in line with current NPCC assurance policies.

-R16. Continue to build cyber defences through the Security Assessment for Policing ('SyAP') and associated security activities.

-R17. Review, streamline, and de-duplicate documentation including service instructions, standards, and policies to ensure they are up to date and in line with the latest NPCC policies, are user-friendly and easily accessible to all who require them.

-R18. Conduct an urgent review of the current GSC policies and application throughout force, including focus on 'SAP' HR System ('SAP') reports, ensuring understanding of the need to classify individual documents, and use effective handling conditions. This should include identification of all PSNI Assets of Official Sensitive or above.

-R19. Determine the on-going need for associated audit mechanism. Ensure the identification, classification, and management (handling, storage, network configuration etc) of force information assets is based on associated risks and value, and consistently applied across the organisation.

7.0 Building the Foundations

7.1 A large proportion of the FOI requests used data from 'SAP'. In all organisations, but more pertinently in PSNI, Human Resources amongst the most sensitive data set held by an organisation.

7.2 Information Technology Security controls are strong, which provide a good foundation to build upon. Within PSNI, there are a number of information security measures that should be applied to all systems including sensitive data as a matter of urgency. Resource and capacity allowing they should be applied to all systems as good practice. Indeed, to do this, it is necessary for PSNI to also fully understand, and effectively manage, the data held within the systems. Earlier recommendations in this report have already touched on this point.

7.3 It was noted during the review that the version of the 'SAP' within PSNI is not a cloud or externally hosted system. It is 'on premise' i.e. PSNI hosted. It is heavily customised. Whilst adapting tools like 'SAP' to ensure that they work properly for an organisation is understandable, care must be taken to ensure that the tool is not so heavily adapted that it cannot be effectively managed by the local IT team or supported by the vendor. If a system becomes out of kilter with versions with those used by other customers of the supplier, it is not within the supplier's commercial interest to cater to one customer. They may choose to stop supporting, which means no more upgrades including security patches. At the very least, the supplier is in a strong position to increase costs. It reduces flexibility or resilience in that fewer people will have the familiarity to work effectively with the system. It can become out-dated and obsolete, in much the same way as a mobile phone does.

7.4 The current version of 'SAP' is nearing the end of its supported life, and this offers an opportunity to identify which product and what configurations are best for the organisation, ensuring that such a critical tool remains supportable throughout its life span. 'SAP' as well as being the corporate HR solution is also used to drive role-based access and therefore has a dual purpose which increases risk.

7.5 The 'SAP' user instruction is limited to a 2-page document which is simply written and concise. It is intended to be read, and adhered to by all personnel who have access to 'SAP' who are obliged to sign a confirmation that they have read and understood the contents. However, there is no process to ensure that users are required to re-read or re-confirm their understanding of these instructions on a routine basis to ensure that they have the latest, most

up to date information and knowledge of the system. Standard Practice would be for an annual review.

7.6 The 'SAP' user instructions contain the following direction, 'All reports downloaded from 'SAP' must be marked in accordance with Government Protective Marking Scheme'. The scheme was retired in 2013 and replaced by the GSC Scheme. The user instruction does require that users complete a number of training modules prior to access being granted, one of which is the 'Information Security & GSC'. The latter document is up to date and provides good guidance on how to assess information to be either OFFICIAL, OFFICIAL-SENSITIVE, or higher. However, there is potential for confusion in referencing an obsolete policy.

7.7 The reports downloaded from 'SAP' do not have a classification automatically applied which creates significant risk in the correct and consistent handling of such reports. The report subject of the data breach did not have a classification applied. The presence of an OFFICIAL-SENSITIVE (or higher) marking could have prompted PSNI personnel to handle the information differently. The downloaded reports are also provided with an automatic file name which is a combination of random letters and numeric characters. This is unhelpful in identifying the reports later and could lead to inappropriate management disposal, storage, and retention. Version control should be used for the same purpose.

7.8 Auditing and monitoring of a system help to identify inappropriate, harmful, and unusual behaviour. It is a standard control that forms part of the Security Policy Framework, and the NPCCs Cyber Security Policy framework. There is a manual auditing process in place to confirm that the users of 'SAP' are operating within their permissions. A number of sensitive records are flagged for alerts if any attempt to access is made. This is a basic auditing approach, but it is workable for the size and complexity of the system. (Removed for Security Reasons). The limitations of auditing did not have an impact on the incident under review, since the activity undertaken was within the authority of the users concerned.

7.9 (Removed for Security Reasons)

7.10 (Removed for Data Protection and Security reasons)

7.11 (Removed for Data Protection and Security reasons)

7.12 The review went beyond 'SAP' to core PSNI systems. Whilst most FOI requests require information from the Human Resources system,

data is regularly downloaded and extracted from all system for different purposes. Risk of accidental or malicious data use or breach is system agnostic, and as all are on the same network, the security of the network is only as strong as the weakest link in the chain; the national 'defend as one' strategy applies not just to the national police service level, but also internally to forces across systems and applications on their network.

7.13 The use of the PSNI network for email purposes is governed by Information Security Standards 1.04 – Email Usage, currently at version 1.5 published in June 2020. At 6 pages in length, it provides a good level of detail for the users of the PSNI network, and its instructions are clear. In the section entitled 'sending email,' users are directed that 'emails generated by PSNI users or IT systems must have the appropriate security classification applied before being sent.' Further guidance on the correct classification is provided in the document as follows: *"xiv) OFFICIAL [PUBLIC] material can be sent to any email address, but this must be for PSNI business only. Users must be aware that sending email across the Internet is not secure and the information could easily find its way into the public domain, for example appear in a newspaper or on a website."*

7.14 It is noted that the publication date of the policy is June 2020, which is outside the review period that would normally be considered appropriate for an organisational policy (12 months). There is no corporate mechanism to flag out-dated policies. The policy also identified some secure email methods to other police organisations which may no longer be appropriate considering the technical developments over that period, i.e., use of the 'PNN' domain for secure email.

7.15 (Removed for Security Reasons)

7.16 Limitations within corporate systems such as 'SAP' have resulted in an unusually heavy reliance on generic Microsoft applications including Excel, and shared drives. There are no user guides, policies or ownership of such generic technologies, and there is an expectation of mastery by users without training of guidance. Due to their use widespread use in society, there appears to be a presumption that all users will be skilled to use the applications in a work environment. The risk is sadly evident in the PSNI data breach of August 2023. The organisation may benefit from a review of the use of spreadsheets across the organisation to see where their usage could be incorporated in to existing applications, including the data warehouse. There needs to be clarity,

ownership, accountability, governance, training and monitoring around these technologies also.

7.17 PSNI would benefit from the development of force wide system standards that align to wider NPCC Blueprint Patterns and identified threats. This includes but is not exhaustive of: anti-malware (to detect, prevent and remove malicious software); cryptography (such as encryption); network hardening (securing security channels between servers, endpoints and other devices, such as firewalls) ;application OS hardening (e.g. securing applications against reverse engineering, tampering or malware attacks); Information systems backup (duplication to mitigate data corruption, deletion or loss); patch management (applying upgrades to security and to improve performance of software or devices); to identify and remove any digital legacy (removal of applications or infrastructure resulting in digital limitation to published blueprint patterns or areas of identified vulnerabilities) and technical 'failsafe' mechanisms for the transfer of information; auditing and accounting; and IT account management. PSNI has 'Control Summary Dashboards' which function like a Baseline Control Set for individual systems cover some of the above standards areas. The contents of the various documents provide a significant amount of direction in secure development. There are however no references to NPCC policy, which could lead to PSNI being out of alignment compared to other police forces and unable to collaborate effectively. PSNI ISU should review the latest NPCC Cyber Security Policies and realign PSNI versions where appropriate, considering any increases in control strength necessitated due to local threat levels. There is a significant amount of guidance, support, and documentation available via NPCC Police Information Assurance Board, and PDS Cyber Services.

7.18 The user of an IT system is often viewed as the weakest link in the security of that system. This is a result of the numerous attack types which focus on the potential for an authorised user to make a mistake, and this provides an attacker with the advantage required to successfully compromise the system. Furthermore, system users can make mistakes in the management of the system, or with data that is produced by it, resulting in its accidental disclosure. Therefore, in concert with routine security awareness and training, it is good practice to ensure that all system users are provided with documentation on how to use that system in a secure manner. The documentation can be provided electronically, or in paper form, and it is usual practice for the user to acknowledge the instructions before accessing the system. This should not however be over onerous.

7.19 The provision of instructions for users to adhere to is a core element of Information security, cybersecurity, and privacy protection, all of which are good practice. Security operating procedures (or similar documents) were identified and reviewed for all PSNI systems reviewed. An expectation for operating procedures is that they are written with a clear focus on the end user, ensuring that everyone is clear of their responsibilities and escalation points.

7.20 Failsafe mechanisms, such as Data Loss Prevention (DLP) , can be useful in ensuring that sensitive data is not transmitted outside of the organisation. Their use is inferred in the Security Policy Framework, whilst also supporting the outcomes of common security frameworks such as NIST and ISO27001. The use of DLP would, assuming a document is properly labelled, significantly reduce the likelihood of an incident of this type occurring. There is a basic DLP operating on the PSNI network. Sensitive information can only be sent to approved domains. In this instance, if the original Excel spreadsheet had been properly classified in accordance with the 'SAP' user instructions, and an enhanced Data Loss Prevention were in place, its transmission as an attachment would have prompted an alert and forced further investigation prior to its release. PSNI policy identifies that email which breach the DLP policies are quarantined, and the assistance of the ISU is required to release them, a situation that would have brought another set of eyes into the situation, increasing the likelihood that the attachment and its sensitive data would have been intercepted. A more advanced capability that would look beyond the classification of the document for key words within would provide an additional level of security if the user had neglected to classify a document or had applied the incorrect classification.

7.21 As part of the review, the access control management for both the core PSNI network and 'SAP' were reviewed. The core network is managed via by the central IT team using role-based access control. This is a method that assigns access permissions based on an end user's role in the organisation. The procedures for adding, deleting, and changing accounts and their privileges are consistent with the standard expected of a policing organisation.

7.22 There are some positive foundations for data management within PSNI that could be further exploited, not least through use of the data warehouse and capitalising on specialist analytical skills and experience. Without building the associated underlying capabilities, the return on investment in technologies and

data security will not be maximised, or the data leveraged for improved insights, better decision making and problem solving, and efficiency. This can be related to many of the initiatives in the digital strategy, in particular projects such as natural language processing, body worn video, video analytics, and augmented Artificial Intelligence. The corporate and cyber infrastructure upgrade, the replacement records management system and the robotics project will be severely restricted by lack of investment in data capabilities.

7.23 PSNI has a functioning data warehouse that is put to limited use and the review team found no knowledge of it outside of Statistics Branch and ICS. A data warehouse is a large store of multiple datasets, where they can be combined and manipulated to produce reports, answer queries or feed various analytical or automated data related processes. They also represent the opportunity to have one 'single version of the truth' across the organisation as opposed to siloed, distinct dataset prone to inconsistency and skewing understanding of the data.

7.24 PSNI reports a comprehensive 'Review, Retention and Disposal' schedule approved by the Northern Ireland Assembly. There is an associated programme of work to implement the policy. There is also some localised yet limited data quality work on-going. The organisation would benefit from further attention in this area to underpin their compliance in such fundamental areas.

7.25 Understanding how effectively data is managed for positive benefit is important, and a data maturity assessment is an important tool for this purpose, particularly if conducted by independent experts providing an objective view. It would highlight current capability and suggest future direction across disciplines such as data management (collection, organisation and accessing), data governance (availability, quality and security), data literacy (ability to read, write and communicate data) and data ethics (moral obligations in collecting, protecting and using data). There are strong interdependencies across these and other fields, including Data Protection, Records Management, Information and Technology Security, data innovation, analytics and Artificial Intelligence. Of course, this is not something that can be achieved overnight. Best practice would lean towards prioritisation of certain elements, such as identifying high risk/ high value data sets, ensuring clear data ownership, and understanding how this relates to Information Asset Ownership, targeting data literacy and getting to grips with data quality.

7.26 Section recommendations

-R20. PSNI should commence the process to identify the replacement or upgrade options for the 'SAP' system, ensuring that the selected product is both appropriate for the organisation but can also be supported through its lifecycle.

-R21. Conduct a risk assessment of the role of 'SAP' in relation to Active Directory.

-R22. (Removed for Security Reasons)

-R23. System controls should be strengthened in relation to 'SAP', and other systems holding personnel data or sensitive operational information. This should include annual resigning of user agreement, review and update of user instructions and policies (including the email policy and alignment to NPCC Cyber policy) , documentation, and capture of tacit knowledge to identify and remove any single points of failure. Consider application of security classification, role-based access control, reports only being downloadable to one system location, minimisation of copies, the application of naming conventions, and regular, robust 'Review, retention, and disposal' regimes. Consider the requirement for increased audit and monitoring.

-R24. Consider the replacement of current Data Loss Prevention software to cover content not just selected metadata / headline classification.

-R25. Participation in the NPCC Digital Data and Technology Coordination Committee delivery boards and associated activities would provide professional support and learning.

-R.26. The PSNI data warehouse should be expanded to incorporate more datasets, have more use cases and users.

-R27. A Data Maturity assessment should be conducted with urgency to understand the organisational position and develop a programme of work, continuously improving and coordinating existing services and building new capabilities including data governance and data ethics. Stakeholders should include information security, records management, data protection, data management, data innovation and data analysts, alongside staff representative of the broader organisation (for example those in operational or corporate roles).

-R28. Work should begin to identify data domains and high risk/high value data sets, and ensuring data owners, clearly defining the responsibilities and relationship with IAOs. Consider a proactive, corporate 'Data Quality'

and ‘Review, Retention and Disposal’ programme, prioritising the high risk/high value data assets.

8.0 Data Sharing and Usage

8.1 Data sharing is essential for policing, be it internally between colleagues or externally with other police forces, partners, or the public. That is the nature of a corporate asset. It is a resource of value held and controlled with the expectation that it will create future benefit. Like people and resources, it is one of the basic commodities used and combined with others to provide services and solve problems. Imagine law enforcement with no criminal records database, a police force with no fingerprints or DNA, or an any organisation without their staff's bank details. Parallels have been drawn with air or water. It is simply a necessity that needs to flow.

8.2 The PSNI data breach on the 8th August was a stark reminder that it is essential to use and share data safely, and the intrinsic difficulties in doing so. Therefore, data sharing must be a priority for any police force and requires clear policy, practice, prioritisation, and mastery. The review team identified a sense of acute awareness of the perils of external sharing, but a similar mindset and practice does not exist when it comes to sharing data within the organisation, including a lack of consideration of malicious and non-malicious insider threats. There are associated policies and training in place, yet there is still a lack of diligence relating to internal sharing in practice. This is seemingly fuelled by confidence in external physical and technical defences. This is in stark contrast to the apparent lack of transparency in relation to officer and staff related matters, such as promotions and transfers.

8.3 There is a level of caution prevalent in PSNI in the security of modern technologies, such as SharePoint, PowerBI, and Microsoft 365. This could result in an overly restrictive culture, depriving officers and staff access to tools with which they can share data safely and reinforce good information security and management practices e.g., Microsoft Purview.

8.4 The majority of interviewees described their understanding of how to extract, minimise and anonymise data and information as being handed down through custom and practise. There are wide variations of practices from department to department, team to team. Barring local good practices identified in the Statistics Branch and Professional Standards, there is little in the way of official policy, process, and guidance. The review team saw evidence of some guidance within the FOI process to remove metadata from files, including personal data. It came to notice that this functionality is not available to all users,

although no written rationale could be identified from policy documentation.

8.5 Existing policies do not emphasise the importance of access control to systems and data when handling sensitive data. Moreover, they do not comprehensively cover how to minimise data processing, anonymise data or identify potentially hidden data. The ICO produces a comprehensive guide on anonymisation, pseudonymisation and on how to disclose information safely, which will provide an excellent source to inform a force policy. Such a policy, procedures and guidance should be developed and introduced expeditiously to reduce the likelihood of error and inconsistency. Information sourcing policies and processes will also enhance efficiency and accuracy.

8.6 There should be a robust communications campaign championed from a senior level. This should be combined with the review of the GSC to ensure officers and staff have a thorough framework to apply. Indeed, policy and guidance in themselves are not sufficient, with education and monitoring also essential components to ensure effectiveness. Functionality can also be restricted in some cases to specified users.

8.7 Staff described a series of "sign off" opportunities within the current approach to FOI requests. With clear definition and a framework as described above, these gatekeeping opportunities could provide further assurance. In addition, it is regrettable that advice to all police forces issued by the NPCC National Police Data Protection and FOI Unit on 2 separate occasions in January 2023 and June 2023 in relation to the use of pdf format for FOI disclosures had not been sufficiently embedded in to the PSNI local FOI process. The advice had been shared with practitioners via email but was applied inconsistently due to the lack of a clear, single approach for process changes and no standard operating procedures. This advice has now been issued by the ICO in light of numerous breaches and was put in place within PSNI as soon as the breach came to light. However, this might not always be an appropriate format as data needs to be reused, so the policy should ensure to include alternatives, and to explain what is most appropriate depending on circumstances and user requirements.

8.8 The PSNI SIRO has also signalled the need for the NPCC to simultaneously share with practitioners and SIRO, and it has been agreed that active consideration will be made to future communications of a similar nature, whilst attempting to strike a balance between sending excessive communications strategically.

8.9 The data warehouse capability provides an additional means to achieve safe and efficient sharing. Bulk data sharing with partners could potentially be automated from a data warehouse, and queries/data extraction could be managed by a central, specialised team. The Statistics Branch would be ideally placed given their expertise and that they are required to adhere to a professional code of practice. With the relevant data sets ingested, this could provide a safe alternative to data sourcing and query running for specific systems, including for FOI. With the adoption of additional tools such as PowerBi, it is possible to manipulate data and create dashboards without any further data extraction, a capability that could be rolled out more broadly than just specialist teams if managed carefully alongside a robust data literacy programme, and with strong data governance.

8.10 It was reported to the review team that it has been a struggle to manage force ISAs due to capacity, and there is a clear lack of formalised and embedded process for either bulk or ad-hoc sharing. Minutes from the Strategic Performance Board from November 2021 also refer to the lack of progress in this area due to resource shortages. A need for information security specialists to be included in the ISA and DPIA processes was also identified. PSNI should ensure their routine inclusion in discussions relating to IT projects, and data sharing with third parties or suppliers to avoid later delays or unidentified risk. The recent ICO audit has identified several areas for improvement. It is recommended that the ICO findings in relation to Information Sharing are implemented.

8.11 Section Recommendations

-R29. Specific policies and guidance should be produced for all whose roles include the downloading and extraction of data, and its sharing both internally and externally to PSNI. This should cover how to safely download and extract data, and include the principles of data minimisation, classification and anonymisation in line with the relevant ICO Codes of Practice. Consider the creation of a 'Knowledge Repository.'

-R30. The use of the data warehouse should be explored for both internal and external data sharing and queries.

-R31. The ICO recommendations should be progressed (Data Sharing/ Governance and Accountability)

9.0 Data Culture, Talent, and Skills

9.1 Culture defines the norm in any workplace. It signifies 'the way things are done around here,' and what is important. It is also common to have sub-cultures that exist across different departments and teams. The review identified a number of aspects that helped to ascertain the culture that exists in the organisation in relation to data, information, security, and assurance. It is not surprising that given the history of the PSNI and the demographics of the communities it serves, there is unmistakable evidence of a strong physical security culture, with unmarked buildings, and officers and staff understanding what personal protective measures to take. However, this is not the case when it comes to information security. This needs to be addressed to demonstrate a real commitment to rebuilding trust both across the organisation and wider public of Northern Ireland. This is a challenge requiring real leadership, commitment, and drive, with a suitable investment in resourcing and practice. It is reassuring to know that PSNI have invested in a cultural audit which, when taken in conjunction with these review findings and recommendations, could result in making a real difference and signalling a continued dedication to progress.

9.2 In terms of general culture, there are practices that may impede the nurturing of expertise and specialism from within the organisation, with an associated negative impact on morale. Interviewees from all departments pointed to the customary practice of generic recruitment and promotion processes at less senior grades, which in turn inhibit career progression and fails to recognise the importance of expertise and experience of those from specialist areas. It was recognised that this approach does not enable staff to pursue a particular career path and may leave some staff feeling undervalued and placed into roles where there is not a suitable alignment of their skills and aptitudes. It restricts the acquisition of specific skillsets. The unique nature of policing and its data, its mission and its complex regulatory environment also hinder the ability to recruit fully equipped professionals, meaning a steep learning curve when attracting senior talent into the organisation. This is not helped by geographical limitations.

9.3 The existence of job descriptions is inconsistent. Whilst some of the teams interviewed had them in place at all levels, notably information security, they were lacking in some areas. Senior positions appear more likely to have a job description, although some need a refresh. They are less apparent in lower grades roles, with many roles being reported as

generic and based on grade alone. Many of those interviewed have an unclear idea of the expectation of their role. There also seems to be a fragmented approach to performance development reviews and clear objectives to orientate, specialise and motivate the workforce. There is evidence through the 'People Action Plan' that this is something the organisation is cognisant of and seeking to improve. The 'People Action Plan' is linked to the 'PSNI People Strategy', and each department contributed to its development and have responsibility to deliver actions in line with it. However, whilst HR reported a local 'People Action Plan' in place, Corporate Information Branch does not have one. As the plan runs throughout the period 2023-24, departments with no local plan in place may benefit from further focus in this area. Local training records are another area of inconsistency which would benefit from effective service-wide management. The review team were advised that all corporate training records should be updated by business areas within SAP yet found evidence of them being held locally.

9.4 In terms of 'data culture' more specifically, this is not well developed. The need for transparency as a police service is also in-line with PSNI values and the Competency Values Framework. There is an apparent perception at all levels that data protection and FOI are a hindrance, and little appreciation of the fundamental impact on public trust by demonstrating transparency and an understanding of the importance people place on the secure handling of their data. It would be beneficial for the 'Here for You' engagement strategy to reinforce the right to participate in shaping policing through FOI. There is no indication of advisory nor scrutiny groups being involved in discussion about the use of their data in analysis or privacy intrusive technologies. This, along with an appreciation of the potential improvements that can be unlocked by the effective use of data, are localised to specialist units, and do not appear to have permeated the organisation to any notable extent. A clear statement from the Chief Constable and senior leaders emphasising the importance of data, information security, data protection, and data governance to all personnel would be impactive, alongside role modelling from IAOs and reiterating the message that it is everyone's responsibility. The role of IAO is key to the whole information governance framework, and often a weak point within policing and beyond. Some organisations have a formalised IAO appointment process, with a 'letter of appointment' from the Senior Information Risk Owner stressing the importance of the role and its status in the organisation. It is also good practice to include professional development objectives specific to the role.

9.5 It is important that the organisation embraces information security into its culture by ensuring that all staff understand their role in protecting the information they handle and its sensitivity. Adequate education and training are also included in Principle 11: Culture of the National Policing Community Security Principles. It is also part of the statutory requirements for a DPO. Indeed, the range of required skills and knowledge are vast, and it is to PSNIs credit that it has in place mandatory e-learning and annual refreshers on induction for FOI, data protection, and information security. Compliance rates are high, and all interviewees attested to having completed them. There is a general sense of understanding that only what is legal, proportionate, and necessary should be shared externally although a lack of understanding of who is responsible for, or who 'owns', the information. The packages are however incredibly detailed and include content that is not necessary in such depth for all, repeating the fine detail of legislation. A case in point in GSC, where it has been highlighted earlier in this report that additional efforts are essential and current training is less effective than is necessary.

9.6 The PSNI Security Branch has a number of good resources to assist officers and staff in managing their personal information in the public domain and protecting against social engineering or triangulation of data for personal identification. It includes for example how to use comparison sites and buy insurance online lawfully without compromising your personal data. From interviews and discussion with the review team, there was limited evidence of widespread awareness of the guidance. There is no doubt that this resource has been shared and is easily available yet its importance appears to be poorly recognised. It is easy for key messages to get lost amongst the vast volumes of service instructions and force wide emails. It is essential that this guidance is promoted further.

9.7 Whilst data permeates all areas of an organisation, the training and skills required is different for everyone depending if they are users, creators, custodians or protectors of data, and what they are using it for. There is some provision of specialist training to IAOs and in specialist roles in information management disciplines. It was reported that the DPO and ISU input has been sought for other training such as induction. It is also acknowledged within the data protection surveys that more bespoke training is desirable, but only provided 'on request'. Training can be extremely effective when embedded as a golden thread through existing products. Leadership training or individual IT system training are excellent opportunities. Indeed, the NPCC Policing

Executive Leadership programme has for the last three years included 'Data' and 'Cyber' within its 'Business Skills' module. Some roles do require a more tailored offer.

9.8 For training to be effective and efficient, it requires an investment in understanding the learning needs of officers and staff. Whilst the PSNI college appears to have little involvement at the current time, those with the task of educating in this arena would benefit from specialist pedagogic support in the development and delivery of a data learning needs analysis, a data literacy framework, and a series of training products. It must be reiterated that PSNI is not in a dissimilar position to other police forces, although many are starting to recognise the need for further investment in this area.

9.9 The roles of SIRO and IAO are fundamental, and obvious for requiring effective training and guidance. The College of Policing offers a one-day SIRO Hydra exercise. PSNI IAO training is currently delivered by the ISU and based on the IAO's handbook. Many commercial training providers provide IAO training but should be carefully chosen as some do not cater for the processing of Law Enforcement data. It is evident that existing IAOs do not have a full understanding of their role, not helped by a rapid turnover and confusion arising for the division of the role into 'Strategic' IAOs and IAOs, which appears to be specific to PSNI and blurs accountabilities and responsibilities. One interviewee reported not having been aware that they were in fact an IAO and disputed that they were the correct person to carry out the role. A further weakness is the responsibility of an outgoing IAO to arrange training for their successor. There has been no consistent national approach within policing to training for these roles. National work is underway that will assist PSNI with resolving this locally.

9.10 Accountability of the Information asset and risk owners is also outlined in Principle 1: Accountability of the National Policing Community Security Principles. NPCC Information Asset Owners handbook (2018) highlighting the importance of ensuring information assets are handled and managed appropriately, stating IAOs must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they can understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process.

9.11 The review team found that specialists working in ISU, data protection and FOI had received specialist training for their roles. They would benefit from exposure to the other disciplines which have some areas of commonality and interdependency. There was evidence of inconsistency in the application of training of FOI decision makers. They follow a comprehensive in-house training plan that is detailed and largely fit for purpose. They would benefit from a more detailed understanding of data protection, which applies by default when applying the section 40 'Personal Information' exemption. Their training plan also includes completion of the NPCC FOI decision maker's course. Many in Corporate Information Branch have completed NPCC data protection training in relation to the processing of subject access requests. More content on identifying hidden data and anonymisation is essential. PSNI is involved in NPCC Cyber training development. Further training and role definition is essential for business areas involved in data sharing, and in FOI specifically.

9.12 Most forces are looking to build data literacy more broadly across the organisation to ensure all data users and creators have the necessary skills to fully understand data, including patterns and trends, and how to do basic analysis. Training and awareness do not need to be resource intensive or classroom based. Modern alternatives should be explored, and a range of options pursued to suit the needs and preferences of individuals. For example, prior to the Covid pandemic, IAOs met regularly to share best practice and problem solve, and these sessions have recently been reinstated. Technology platforms also provide an excellent opportunity to spread knowledge and build enthusiasm through a 'crowd sourcing' approach using communities of practice or networks of champions. Progress can then become organic and self-perpetuating.

9.13 Section Recommendations

- R32. Explore the possibility of non-generic recruitment and promotion within the FOI area and the areas of information management and security, recognising the specialist nature of the roles and requirement to build experience and expertise as a means of creating resilience across the organisation and high performing teams.

- R33. Consider the identification of data roles and responsibilities on bespoke role profiles and associated regular objectives and development reviews.

- R34. The PSNI college should work closely with the relevant teams to conduct a Learning and Training Needs Analysis across the organisation,

including specialist data roles, with a view to then developing an adapted, targeted set of learning products. Due to the heavy reliance on Microsoft Excel, this should form part of the analysis.

- R35. Following the Learning Needs Analysis, a differentiated and role-based bespoke force-wide Data Literacy Programme should be developed, identifying the role of the college and stakeholder departments. Consideration should be given to where data and information disciplines can be included in existing programmes as a golden thread e.g., leadership courses, IT courses, and what bespoke products should be developed and delivered in priority order. Consider the establishment of 'Communities of practice' and 'champion' networks across force.

- R36. Comprehensive, accurate and detailed training records should be held and managed at a corporate level.

- R37. There should be visible executive level support for transparency, information security, risk management, and associated business areas. Consider an executive level sponsored organisational awareness campaign including explaining the value of FOI, the message that information security and management is everyone's job, and of the importance whilst on and off duty.

Appendices

Appendix A: Terms of Reference

INFORMATION SECURITY AND GOVERNANCE

Independent Review

Systems, Policy, Processes, Practice, Culture & Behaviors - in response to the Data Breach Incident of 8th August 2023

TERMS OF REFERENCE

1. Introduction

This Review has been *jointly* commissioned by the Northern Ireland Policing Board (NIPB) and the Chief Constable of the Police Service of Northern Ireland (PSNI) into the circumstances surrounding an information security data breach incident on 8th August 2023 that led to disclosure of personnel records to '*Whatdotheyknow.com'* public website in response to a routine Freedom of Information (FOI) request.

This Review will be led independently of the NIPB and the PSNI and is designed to:

(1) Investigate (a) the processes and actions that led to the breach occurring and, (b) any organisational, management or governance factors that allowed that breach to occur.

(2) Identify any action required to prevent further data leaks, to build more robust future risk mitigation systems and to make recommendations for any necessary improvements to information governance systems, policy, organisational practices, cultures, and behaviours; and

(3) Restore confidence in the organisation's approach to information security.

Note: C*onsequence management* relating to the immediate information security actions, incident investigation and personnel security and welfare matters following the specific incident continue to be governed separately via Gold Command critical incident response under Operation Sanukite.

2. Background

On 8th August 2023, the Police Service of Northern Ireland (PSNI) suffered a critical information security data breach following a routine Freedom of Information (FOI) request. Data contained within a spreadsheet was published on a legitimate website called www.whatdotheyknow.com.

The detail was formatted into thirty-two (32) columns including the surname, initials, rank/grade, role, service number, department, location, duty type and gender of all serving officers and staff.

Due to the sensitivity of the information, as well as the ongoing SEVERE threat level, a Critical Incident was declared on the 9th of August 2023, with reporting into (PSNI) Platinum and Gold Command structures.

This loss of information has caused unquantifiable damage to the confidence of officers and staff in the PSNI, as well as in the eyes of the public and the PSNI's policing partners, as to the capability to handle personal and sensitive data safely and securely. As result, this Independent Review has been commissioned.

The Senior Responsible Officer (SRO) undertaking this Independent Review will report directly to the Chair of the Northern Ireland Policing Board (NIPB) and the Chief Constable of the Police Service of Northern Ireland (PSNI).

A summary of the governance structure for the Independent Review is attached at **Appendix I** for reference.

3. Scope of the Independent Review

The **objectives** of the Independent Review fall under the following key themes:

Processes and Protocols

1. To review the workflow processes in place at the time of the breach, establish compliance against any documented Standard Operating Procedures and/ or agreed processes or policies.
2. To identify the root cause(s) of the information security breach and record any learning.
3. To review the current process for handling FOI requests against compliance with the 'NPCC FOI Manual of Guidance' and the 'ICO Guide to FOI' and make recommendations.
4. To identify business areas that handle large volumes of sensitive personnel data that are routinely requested under FOI and the IT systems that support those processes.
5. To review current information security and data handling steps (including accountability, quality assurance, system limitations, access permissions and information security standards) for those processes and systems identified in point 4.
6. To inform options for mitigating risk of future information security incidents for those processes and systems identified in point 4.

Policy and Systems:

For those systems identified under point 4 above:

7. To review Standing Operating Processes and any other internal policy, guidelines, service instruction(s) or standard(s) particularly where there are instructions for the extraction of data, attaching of documents and the application of controls to data released to third parties.
8. To review the assurance documentation, identifying any gaps in assurance or residual risks that are relevant to the breach.
9. To review the development of standards for these systems, comparing to required.
10. To review existing auditing and monitoring capabilities.
11. To review controls/ alerts and presence of any technical failsafe mechanisms in place relating to the transfer of information and options for further development.
12. To examine and provide advice on any changes to information security requirements/access permissions and controls.
13. To provide advice on updated Security Assurance for Policing ('SyAP') scores where appropriate.

People - Culture, Practice and Behaviours:

14. To review the skills sets required and/or training needs and status for personnel involved in data sharing functions.
15. To assess attitudes and behaviours surrounding the robustness of organisational information management practices including evidence of proportionality of data sharing.
16. To examine lines of accountability, governance, and oversight in information management roles.
17. To review adherence to legal obligations.

4. Governance

In order to ensure that the Review has the appropriate powers to complete a thorough investigation, a partnership has been agreed between the Northern Ireland Policing Board (NIPB) (as the accountability body) and the Chief Constable of the Police Service of Northern Ireland (PSNI) (as the body with operational responsibility).

The Senior Responsible Officer (SRO) for the Independent Review is **Assistant Commissioner Pete O'Doherty**, NPCC Lead for Information Assurance. The SRO will be supported by a Review Team that

includes a number of specialists that work for both Police Digital Services and the National Chief's Police Council. The members of the team provide extensive skills and experience in freedom of information requests, information and cyber security, data protection and compliance.

The Chief Constable, the NIPB and the Review Team will develop procedures to protect personal information of individuals (including officers and staff) and ensure that confidentiality of information is maintained during the Review period and in the Report.

5. Leadership of the Review

The Review will be led by the SRO as outlined at Section 4 above. Designated Single Points of Contact ('SPOC') for all matters of logistics and support to the Review Team are as follows:

- **Aldrina Magwood, ACO Strategic Planning & Transformation - PSNI**
- **Sinead Simpson, Chief Executive - NIPB**

A PSNI corporate support team will be established to facilitate and enable the work of the Independent Reviewers.

In addition, the Department of Justice (DOJ) will provide critical peer support as required.

The NIPB and the PSNI will provide access to the following as are relevant to the scope of the Review:

a. Policies and systems.
b. Related training material.
c. External and internal risk, assurance, and audit reports.
d. Briefings from key staff in relation to the above.
e. Other requests or access to staff to be agreed.

6. Methodology & Timescales

The Review Methodology will assess against relevant sections of established professional and expert standards, including police standards, and best practice.

Standards will include, but not be limited to, College of Policing Information Management APP, NPCC published standards and Manuals of Guidance, and policing security standards. The review may also have regard to broader relevant standards such as ICO and government Digital Data and Technology (DDaT).

'Best practice' is what has been established as such by the NPCC DDaT Coordination Committee and sub portfolios, the expert National Police FOI and Data Protection Unit, and the Police Digital Service

(PDS) Cyber and Data Units. The Review will also simultaneously be working closely with the NPCC National Police Data Board to identify any further good practice of relevance.

It is expected it will be necessary to conduct a phased Review to deliver the full scope of the objectives commissioned.

- **Phase 1** – will commence 29th August 2023 and will deliver the objectives relating to the specific data breach incident of the 8th August 2023. This Phase will be completed on the 8th September 2023 and will include Stages 1 and 2.

The outcomes of Phase 1 will further inform the Review Plan proposed to deliver fully the objectives agreed as part of Phase 2.

- **Phase 2** – will run sequential to Phase 1 and will involve Stages 3, 4 and 5. Phase 2 is estimated to be completed by the 30th November 2023

The Review will be conducted in five (5) stages:

Phase One – Discovery

Stage 1 – (21st August 2023 to 28th August 2023):

- Logistics
- Documentation
- Interview and observation schedule
- Commencement of online research

Stage 2 – (29th August 2023 to 8th September 2023)

- Request of any further documentation considered relevant by the Review Team.
- Undertake interviews[1] and observations as agreed, and as may become necessary throughout the Review.
- Continued online research.
- Any high risk finding requiring immediate action will be notified as soon as possible and where possible, be reported to PSNI Gold Command.
- 'Hot debrief' and sharing of high-level findings with the NIPB and the PSNI. This will include an overview of any high-risk findings notified through the PSNI Gold Command structure.

By the end of Phase One and to ensure procedural fairness the Independent Review Team will establish and provide the facts required to enable the appropriate authority within the PSNI to make a determination if any disciplinary procedures should be initiated.

Phase Two - Report Preparation & Reporting

Stage 3 – (September to October 2023 plus 2-weeks for slippage)

- Review Team review and write-up of findings.
- Research into current best practice amongst Home Office Police Forces will be conducted to further inform recommendations.
- In writing the Report, the principles of FOI with be applied to the Main Report intended for future publication. Any findings not suitable for public disclosure will be prepared for sharing with the NIPB and PSNI in closed session.
- Follow-up of any significant action taken in the period since the review and high risk, immediate findings reported as part of the site visit.

Stage 4 – (Estimated Mid November 2023)

- Review of factual accuracy with relevant parties
- Consultation with relevant parties in relation to establishing any harm to inform the decision making for inclusion in the 'closed' report in line with FOI obligations.
- Finalisation of the publication date
- Final draft of the Report by the Review Team

Stage 5 – (estimated End November 2023)

- Final version of the Report presented and released to the NIPB and the PSNI.
- Consideration of requirement for any follow up.

Delivery against the timeline will be subject to availability and access to all relevant information.

7. Deliverables

The key deliverables of the Review to the Northern Ireland Policing Board (NIPB) and the Chief Constable of the Police Service of Northern Ireland (PSNI) include the following:

- Regular feedback on findings as the Review progresses.
- A Draft Report, enabling both parties to provide comment.
- A Final Report.

In conducting the Review, the Reviewer will comply with all applicable laws, including in relation to personal information.

8. Publication

The Final Report will be published.

The Northern Ireland Policing Board (NIPB) and the Chief Constable of the Police Service of Northern Ireland (PSNI) will be provided with an un-redacted copy of the closed findings subject exempt from disclosure under FOIA if applicable.

The details of the report will be kept confidential until both parties decide on the publication arrangements. The Permanent Secretary or Minister for Justice (subject to any return to the NI Assembly) will be advised of publication arrangements and provided with a copy of the Report.

[1] The Review Team will undertake all interviewing in a sensitive manner and in-line with the wellbeing and welfare objectives of the PSNI. Noting that establishing the full facts of the data breach is dependent upon the cooperation of the organisation's employees.

Appendix B: Methodology

The terms of reference for the review set out the overarching approach.

Interviews and group discussions took place with more than 50 PSNI officers and staff of all levels, and members of the Northern Ireland Policing Board. Within PSNI, this included: The Chief Constable, Deputy Chief Constable, Chief Operating Officer and members of the Senior executive Team, PSNI Senior Information Risk Owner and Silver Commander for Op Sanukite, Staff associations and minority groups, Information Asset Owners, Operations Support Unit Senior Management and staff from Corporate Information Branch, Information Security, Records Management, Data Protection, Data Quality, Information Sharing, Security Branch, Human Resources, Information and Communications technology, Human resources, Corporate Services, Statistics Branch, Finance, Audit and Risk Management, Professional Standards and Strategic Communications and Engagement department. The review team spoke to all individuals who had direct involvement with the Freedom of Information request that led to the data breach.

In addition, over 20 representatives from UK police forces contributed to four sessions conducted by the NPCC National Police Data Board in relation to identifying standard and good practice across the service.

The Department of Justice (NI) provided peer review, and the Cabinet Office participated in the review of the report to determine applicable redactions from the public facing report alongside expertise provided by the NPCC National Data Protection and Freedom of Information Unit.

The review team has expert knowledge of relevant legislation, industry, and policing standards such as the Community Security Policy, Government Security Classification and College of Policing Approved Professional Practice, and regulatory codes of practice and guidance. The team were selected for their extensive and expert skills and knowledge, alongside consideration of a balance of independence, and understanding of policing data, technologies and compliance and regulatory environments.

More than 200 individual NIPB and PSNI documents were recovered and reviewed, including:

Information Security Incident reports
Freedom of Information request records
Individual statements
Incident timelines
FOI process documentation and templates
Service instructions and policies
PSNI Standards Documents
FOI Service Instruction
Training records
E-learning including all mandatory staff induction modules, and bespoke modules for FOI staff
Locally developed guides
Records of interviews and group discussions
Organisation strategies
Minutes and reports from meetings including NIPB, Strategic Management Board, and Information Governance Group
Advice leaflets
Organisational Structure and corporate governance charts
Job descriptions
System user instructions, user agreements, and security accreditation documentation
Risk Registers
Internal audit plans and reports
Business Continuity plans
Performance reports
Audit trails
Policy development guidance
Business cases
ICO audit documentation
Op Sanukite decision log
Parliamentary Select Committee transcript

Action plans
People plans
Call logs
Information Sharing Agreements

Appendix C: Review Team profile

The team was composed as follows:

T/Commissioner Peter O'Doherty – City of London Police – SRO

Claire Vickers-Pearson – Head of Data and Information, West Yorkshire Police, Deputy SRO

Review Team Member 1 - Police Digital Service (Data).

Review Team Member 2 – National Police Freedom of Information and Data Protection Unit

Review Team Member 3 - Police Digital Service (Data)

Review Team Member 4 - Police Digital Service (Cyber)

Review Team Member 5 - Police Digital Service (Cyber)

Review Team Member 6 - Police Digital Service (Cyber)

The multi-disciplinary review team combines years of expert knowledge, skills, and experience across a vast range of sectors and disciplines, working with multiple and wide-ranging partners at national, regional, and local levels. They are all currently practicing across various UK police forces, National Policing Units, and the Police Digital Service Data and Cyber services.

Experience includes:

- Policing roles in operational enabling service and functions (Police Officer, Safeguarding, Public Protection, Digital, Disclosure)
- Public Sector roles in the Armed Forces, National Health Service, Regulatory Bodies, Civil Nuclear Sector, and Home Office.
- Private sector roles Telecoms, Finance, and Cyber.
- Private consultancy.

Relevant qualifications include: ISO 8000, M(Sc) Information Security, Chartered Cyber Security Professional, Certified Information Systems Security Professional, Certified Information security manager, certification in Information Security Principles, ISO27001 Information Security Auditor, National Institute of Standards and technology Professional, BCS Data Protection and GDPR, BSC Freedom Of Information, Cloud Security Alliance Certificate in Cloud Security Knowledge, Chartered

Institute of Information Security. BCS Certificate and Lead Auditor specialising in ISO/IEC 27001, ISO/IEC 20000-1, ISO 22301, ISO 9001, and APACS Standard 55 (CPAS).

Specialist disciplines:

Freedom of Information, Information and Cyber Security and Assurance, Cyber and Data Breach Management, Data Protection, Operational Security, Data Strategy, Data Maturity, Data Quality, Data Governance, Data Management, Data Science, Data and Information Sharing, Data Analytics and Visualisations, IT System Management, Policy and Standards, Training, and Audit, Inspection, and Risk Management.

Partnership working across:

National Police Chief's Council. Government Departments including Home Office and Cabinet Office, Security Services, Counter Terrorism Policing, Information Commissioner's Office, Investigatory Powers Commissioner's Office, Office of the Surveillance Camera Commissioner, UK Accreditation service.

The team includes a visiting professor in Cyber from a UK University, experienced major cyber incident decision makers, members of a number of NPCC DDaTCC sub boards including the NPCC Police Information Assurance Board, and the NPCC National Police Data Board.

Appendix C: Glossary

Term	Definition
ARAC	Audit and Risk Assurance Committee
Cyber Security	The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
Dark web	Areas of the internet that are not easily available to the general public, and are often used for criminal or terrorist activity.
Data Breach	Exposing confidential, sensitive, or protected information to an unauthorised person(s).
Data Management(DM)	The process of organising, storing, and using data in a way that meets the needs and goals of an organisation. Data management involves techniques and tools to ensure the quality, security, accessibility, and usability of data.
DDaT	Digital Data and Technology
DLP	Data Loss Prevention
DP	Data Protection
DPA	Data Protection Act
DPO	Data Protection Officer
FOI	Freedom of Information - References activities under the Freedom of Information Act(FOIA)
Freedom of Information	Providing public access to information held by Public Authorities
GDPR	General Data Protection Regulation
GSC	Government Security Classification
IAO	Information Asset Owner
ICO	Information Commissioner's Office
ICS	Information Communication Services
IGDG	Information Governance Delivery Group
Information management	The collection, organisation, storage and maintenance of data
ISA	Information Sharing Agreement
ISU	Information Security Unit
IT Security	The protection and processing of information by technical means
KPIs	Key Performance Indicators
NIPB	Northern Ireland Policing Board
NIST	National Institute of Standards and Technology
NMC	National Monitoring Centre
NPCC	National Police Chiefs Council
OS	Operating System
PDS	Police Digital Services
Power BI	A technology-driven business intelligence tool provided by Microsoft for analysing and visualising data.

Records Management	Supervision and administration of digital or paper records, regardless of format.
Register of processing activity	A document or system that holds Information about the use of personal data.
Risk Register	A risk management tool that is used to identify potential risks.
SAP	Human Resources System
SIRO	Senior Information Risk Owner
SOP	Standard Operating Procedure
SPOC	Single Point of Contact
SRO	Senior Responsible Owner
SyAP	Security Assessment for Policing