HEDDLU GWENT POLICE

Information Services & Governance

Annual Report

2022/23

1. PURPOSE AND RECOMMENDATION

1.1 The report presents the annual outturn on the delivery of Information Services, Information Governance and Information Security in Gwent Police.

1.2 There are no recommendations made requiring a decision.

2. INTRODUCTION & BACKGROUND

2.1 In response to the introduction of the General Data Protection Regulations (GDPR) in 2018 the force established the Information Services and Information Governance structures, both of which report to the Assistant Chief Officer – Resources.

2.2 The Information Governance structure is headed by the Joint Data Protection Officer (DPO) shared with South Wales Police. This role is focussed on meeting the requirements of the GDPR and the Data Protection Act 2018. The structure of the Information Governance Team preserves the independence of the DPO as required by legislation. In addition, it also brings together complementary processes to ensure compliance when dealing with information across the force.

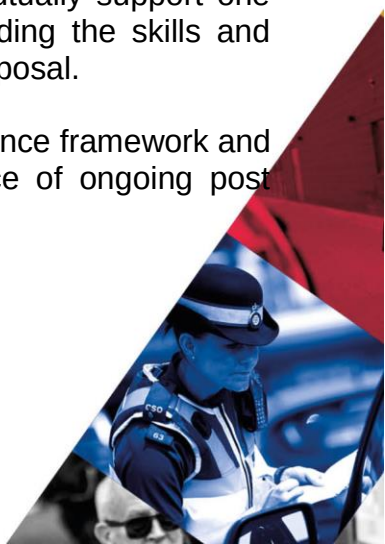
2.3 The Information Services structure is headed by the Head of Information Services and provides disclosure on data management provision for the force in line with legislative requirements. Other services provided include Police National Computer (PNC) maintenance and Firearms Licencing management.

2.4 This report presents the key performance areas for both Information Governance and Information Services. These are monitored through the Information Assurance Board (IAB).

2.5 An Information Management Collaboration Project (Gwent and South Wales Police) has undertaken a review of both Information Services and information governance functions (Phase 1). The organisational structures, policies and processes within each force were reviewed and recommendations were made to the respective Governance Boards. The business case was approved in November and implementation commenced in January 2023.

2.6 A mirrored collaborative structure has been implemented; effectively managing organisational risk and aligning structures that mirror each of the business areas across both Gwent and South Wales Police. In doing so, both forces are adequately resourced in managing demand, providing an opportunity to mutually support one another and enabling business continuity. Aligning and extending the skills and knowledge across the teams was an essential element of this proposal.

2.7 To ensure effectiveness both forces will utilise the same performance framework and maintain regular monthly meetings together with the assistance of ongoing post implementation reviews.



2.8 The project has achieved outcomes of aligned processes, joint policies and procedures, a wider network of skills and knowledge, efficiency gains across the business functions, compliance with legislation, reduced risk to our communities, improved succession planning, collaborative working, improved resilience and leadership structure, improved business continuity and demand sharing together with the ability to mutually support one another.

2.9 Phase 2 of the Information Services review has commenced; to include PNC/Law Enforcement Data Service (LEDS), Warrants, Road Traffic Collision disclosure and Disclosure & Barring Services.

2.10 The Information Security function is delivered by the Force Information Security Officer (FISO) who also reports to the Assistant Chief Officer – Resources, the Senior Information Risk Owner.

3. ISSUES FOR CONSIDERATION

3.1 The reporting arrangements have been operational throughout the financial year.

3.2 INFORMATION SERVICES - DISCLOSURES

3.2.1 The disclosure categories and performance are summarised below with supporting explanation and the detailed performance analysed at Annex 1 for Subject Access and Freedom of Information. This is also published on the NPCC website.

- Subject Rights Provisions
  - Right of Access (Subject Access Requests)
  - Right to be Informed
  - Right to Erasure
  - Right to Rectification
  - Right to Restrict Processing
- Freedom of Information (FOI)
- Environmental Information Regulations (EIR)
- Children and Family Court Advisory & Support Service (CAFCASS)
- Road Traffic Collision (RTC) Disclosure
- Criminal Injury Compensation Authority (CICA)
- Family Court Orders
- Data Protection requests
- Common Law Police Disclosures
  - Notifications
  - Disclosures
- Local Authority Safeguarding Checks
- Disclosure and Barring Service (DBS)
- Police National Computer (PNC)
  - Creation
  - History

3.2.2 Subject Rights Provisions

i. *Right to be Informed*

Individuals have the right to be informed about the collection and use of their personal data. Data Controllers must provide certain information, such as purposes of processing, retention periods and data processors. This information is set out within the Corporate Privacy Notice.

ii. *Right of Access Rights or Subject Access Rights (SAR)*

The SAR service involves the processing of requests from Data Subjects wishing to access their personal data. This can include conviction data, non-conviction data, body worn video and custody interviews.

SARs must be responded to within one month unless an extension is applicable. Performance fluctuated throughout the year, the lowest being 84%. 100% compliance was met for six of the 12 reporting months. The force average for the year was 92%. The national average was 68%.

iii. *Right to Erasure*

GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. There were 19 requests in the reporting period, all processed within the statutory timescale.

iv. *Right to Rectification*

GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. There were three requests in the reporting period, all of which were processed within the statutory timescale.

v. *Freedom of Information (FOI) Requests*

The FOI service involves the processing of requests from members of the public and the media for information held by the force.

The performance for the year fluctuated from a low of 63% to a high of 87%. The statutory compliance rate is 90%. The national average for all forces was 76%. There are two factors that affect performance: capacity within the FOI team; and capacity within business areas to provide responses. The FOI team is currently fully staffed. There is a mechanism to chase outstanding requests and overdue requests (categorised by business area) which are reported via the Information Assurance Board (IAB). The demand and performance analysis are detailed at Annex 1 for information.

The force has a publication scheme and this is provided on the force website at the following link: **Published items | Gwent Police**

In March 2022, the Information Commissioner's Office (ICO) published a follow-up report based on their thematic report issued in 2020 entitled 'Information Access Request Timeliness' in relation to SAR and FOI compliance. There were nine recommendations in total, aimed at driving compliance with the statutory time for responding to information access requests.

A re-assessment against the recommendations has been completed, indicating that Gwent is achieving 'Substantial Assurance' in eight of the quality areas, and 'Reasonable Assurance' in the remaining area. The one area deemed to require improvement related the volume of requests sat with other departments exceeding the specified time for response, and the delays incurred waiting for single point of contract (SPOC) approval both of which have subsequently been addressed.

As a result of high-profile misconduct cases involving serving Police Officers, and Baroness Casey's report on misconduct (Metropolitan Police Service), there has been a national surge for FOI requests in relation to Police misconduct. This has placed demand on both the FOI team and the Professional Standards Department in terms of analytical capability. This is demonstrated by the noticeable increase in requests during January and March. The PSD team are working on the development of datasets for the Force Publication Schemes, facilitating the application of qualifying exemptions in some instances, to manage demand more effectively.

vi. *Children and Family Court Advisory and Support Service (CAFCASS)*

CAFCASS is an independent arbitration service representing children in Family Court. These include public and private law cases. The function includes the provision of Police National Computer (PNC) review and also locally held Police information. Disclosure is required within 5, 10 or 15 days depending upon the level of check required. There were 668 requests during the reporting period.

Performance has been at 100% compliance throughout the year.

vii. *Road Traffic Collision Disclosures (RTC)*

Requests fall into five main categories:

- Motor Insurance Bureau (MIB) - disclosures for untraced drivers
- Association of British Insurers (ABI) - validating insurance claims
- Search requests - insurance claims
- 3rd party requests
- Other - primarily requests for OIC reports

There are key performance indicators for MIB requests (20 working days) and ABI requests (30 working days), all other requests are dealt with subject to demand and capacity. This is a high demand area and there are mechanisms in place to ensure performance is monitored. During this reporting period, a temporary resource has been approved to assist with the accrual of disclosure requests for RTC information. There were 879 recorded requests during the reporting period.

ix. *Criminal Injuries Compensation Authority (CICA)*

This involves the processing of requests and provision of information to CICA, who handle requests on behalf of injured parties. There were 743 recorded requests during the reporting period.

Performance has been at 100% compliance throughout the year.

x. *Family Court Disclosure* (Court Orders)

This involves the provision of Police held information as detailed in the Court Order, relating to private and public law matters.

Performance has been at 100% for eleven months of the reporting period, with only one Court Order returned overdue throughout the year.

xi. *Data Protection / Disclosure*

This involves general disclosure matters and information sharing with regulatory bodies and partners. There is no specified timescale to respond to these requests. There were 350 recorded requests during the reporting period.

xii. *Common Law Police Disclosures (CLPD)*

This involves disclosures to regulatory bodies or employers in respect of nominals that have been arrested/charged for a recordable offence where they are considered a risk to children or vulnerable adults. There is no statutory timescale but there is a local target of 72 hours in which to disclose. There were 924 recorded requests during the reporting period.

Performance averaged 99% for the reporting year.

xiii. *Safeguarding Checks*

This is the provision of information to local authority safeguarding teams in respect of risk assessing children and vulnerable adult placements. The recording of requests changed from *number of nominals* to *number of requests* to align with South Wales Police as part of the collaborative approach. Therefore, the estimated requests totalled 3,302 over the reporting period.

Performance has been at 100% compliance throughout the year.

3.2.3 The disclosure demand is summarised below across the last two financial years. Whilst demand is steady, the complexity of the requests is creating an increasing demand on the teams.

Disclosure Type	Performance Target	Number 21/22	Number 22/23	Change %
Subject Access Requests	One calendar month	325	297	0.91
Freedom of Information	21 Days	1,050	976	0.93
CAFCASS	Stages 1-2(b): 5/10/15 wkg days	738	668	0.91
RTC Disclosure	Various	815	830	0.95
RTC MIB	20 days	Incl above	31	
CICA	30 & 60 days	701	743	1.06
Court Orders - Private	10 days	106	134	1.26
Court Orders - LA	10 days	477	503	1.05
Data Protection Misc	No specific time	230	350	1.52
CLPD	Three working days	847	924	1.09
Safeguarding	10 working days	5,969	5,783	0.97
Custody Records and Interviews	No specific time	287	230	0.8
Total		**11,545**	**11,469**	**0.99**

3.2.4 *Disclosure Barring Service (DBS)*

The DBS team is externally funded and process all DBS applications for the Gwent area. These include:

- initial research of force systems;
- recording of information onto the Quality Assurance Framework;
- disclosures;
- handling disputes;
- ID fingerprints; and
- referrals to Barring.

Performance is measured in terms of timeliness and productivity. In the reporting period incoming demand was 34,947 checks which averaged 14% above forecast demand. The service standard for completing work in progress is 12 days; the force averaged 6 days. In terms of the percentage of checks completed within 15 days, the force achieved 87% against the service standard of 65%.

3.2.5 *Police National Computer Bureau (PNCB)*

The PNCB team maintain PNC Name and Vehicle updates including entering new records, managing alerts, updating current records and deleting records upon request, court resulting, impending prosecutions, and warrants administration. The team is also responsible for inputting Road Traffic Collision injury reports onto the mapping service (AccsMap) and provide RTC statistics to Welsh Government.

Performance in respect of Arrest Summons Creation averaged 89.5%. The target is 90% within 24 hours. The national average was 86.4%.

Performance in respect of Disposal History updates averaged 82.2%. The target is 75% within 10 days. The national average was 84.9%.

3.3 FIREARMS LICENSING

3.3.1 The Firearms Licensing Unit consists of the Administration team and the Firearms Enquiry Officers (FEO). Since January 2023, the unit has also been supported by a Police Constable.

Tasks include services involving the granting of certificates which are:

- renewals, variations, transfers, clubs and registered firearms dealers;
- explosive certificates;
- vetting and medical process;
- suitability and security visits / telephone assessments.

3.3.2 The Firearms Licencing Unit were part of Phase 1 of the Information Services Collaboration with South Wales Police. Significant progress has been made in the financial year and the achievements include:

- An agreed increase in resourcing, notably an uplift of 3 x FEOs and a Police Constable.
- Core systems and processes are now aligned with South Wales Police, utilising the Niche records management system as the primary system for tasking activity and monitoring compliance.
- A joint policy/procedure has been published to underpin our processes and commitment to public safety. The processes are compliant with legislation but also efficient.
- Gwent has made significant changes to the security vetting process ahead of the changes to the statutory guidance and the draft Authorised Professional Practice.
- Risk management is conducted via the Niche risk board where certificate holders, storage locations and home addresses are flagged. This is replicated on STORM (System for Tasking and Operational Resources Management) logs for incidents that are not processed onto Niche, enabling the Firearms Licencing Unit to effectively monitor all certificate holders that come into contact with Gwent Police.
- Social media checks are being conducted for all grant applications and intelligence led checks for renewal certificates and certificate holders who come to the attention of the police are also undertaken.

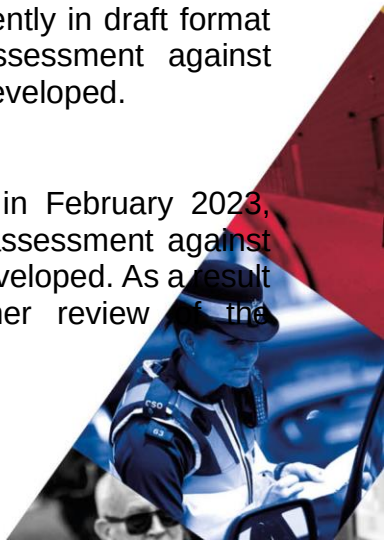
Since the response to the Plymouth shootings, the Delegated Authority in respect of refusals and revocations of licenses remains with the Assistant Chief Constable (ACC), and a temporary Inspector remains in post.

3.3.3 <u>Authorised Professional Practice (APP)</u>

The APP for Firearms Licensing has been revised and is currently in draft format pending the outcome of the consultation process. An assessment against requirements has been undertaken locally and an action plan developed.

3.3.4 <u>Statutory Guidance</u>

The statutory guidance for Firearms Licensing was revised in February 2023, following the public inquiry into the Plymouth shootings. An assessment against requirements has been undertaken locally and an action plan developed. As a result of procedural changes, it has been agreed that a further review of the



demand/resources profiler is undertaken to ensure adequate capacity to comply with statutory guidance.

3.3.5 Governance

Overall performance and risk are reported to the Information Assurance Board and via the ACC, as per statutory guidance. A collaborative Firearms Licensing Steering Group is planned with South Wales Police to ensure alignment is maintained.

3.4 INFORMATION GOVERNANCE

3.4.1 The introduction of GDPR and the UK Data Protection Act 2018 (DPA) has required the organisation to enhance reporting arrangements in relation to the following:

Data Breaches

In the reporting year 2022-23 there were 62 data incidents reported to Information Governance but none have been considered high risk requiring reporting to the Information Commissioners Office (ICO).

The incidents have been assessed for impact as follows:

GREEN	= 38 - (impact on data subject is minimal)
AMBER	= 16 - (subject suffers some damage or distress)
RED	= 0 - (impact on data subject is significant)
No Breach	= 8 - (conclusion of no breach following assessment)

Right to be Forgotten

There have been no requests under GDPR for the Right to be Forgotten. The Right to be Forgotten does not apply to law enforcement data.

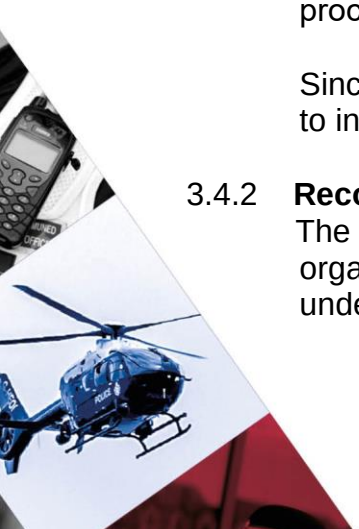
Records of Processing

As part of GDPR/DPA there is a mandatory requirement for the Data Controller to maintain a record of processing activities. Whilst this is linked to the established Information Asset Register regime, the way in which Police systems are used means that a separate record has been established in the Information Governance team who work with departments to document all processes involving personal data, the lawful basis, recipients and sources, security measures and categories of data. This is undertaken through data mapping and will assist the controller in maintaining awareness of where data is collected, processed, stored and protected and which information is being managed by third parties and suppliers (data processors). Controller and processor obligations are also embedded in the contract and procurement process, with data sharing agreements established.

Since the introduction of GDPR/DPA, Gwent Police's compliance has been subject to internal audit and found to be operating effectively.

3.4.2 **Record Management**

The Records and Compliance team provide advice and support to ensure that the organisation is compliant with Data Protection legislation. The programmes undertaken in 2022/23 are summarised below:



i. *Review of Physical Data/Retention*

- **Interview Tapes:** the Records team are continuing to review interview tapes, video tapes and DVDs stored across the Gwent Police estate. Following a review/destruction process the retained items will be secured in long term storage.

- **Digitisation Work/old HQ Decant:** remaining paper files are being scanned to ensure that all paperwork held in the old HQ will be digitised.

- **E-mail Retention:** the policy has been implemented at 12 months retention and the email archive has been finalised alongside a review of the functionality of eDiscovery in Microsoft 365 (M365). Additional apps are being rolled out and retention periods are being implemented incrementally for long terms storage with a migration plan approved by Chief Officers.

- **Gwent Police Retention Schedule:** the Records team continue to monitor compliance with the Retention Schedule during the data mapping process. This will also form part of the ongoing M365 migration work.

ii. *Review of Information Sharing Agreements (ISA)*

All departments are engaged to review the existing ISAs and update or develop new agreements where the data mapping process is identifying new requirements.

Through this process Information Sharing Agreements identified for renewal are summarised below:

Agreement Type	*Completed*	*In Progress*
Information Sharing Protocols	8	5
Data Processing Agreements	2	0
Memo of Understanding	2	2
Data Disclosure Agreement	1	0
Data Protection Impact Assessment	5	9

iii. *Review of Processing Activities*

The Compliance Officer has been working with Procurement to develop a plan to audit our third-party processing activities. This is an area that we have historically not undertaken but is a requirement of GDPR legislation and would form part of any future ICO audit.

iv. *Microsoft 365*

Information Governance continue to be part of the Digital and Agile Project Team delivering the migration of Microsoft 365 across the organisation.

A progress summary is shown below:

- The project continues to be on track with the plan.
- The creation of corporate SharePoint sites is complete.

- The development of metadata and retention policies for legacy data is ongoing.
- The testing of file conversion of legacy documents was successful.
- The migration of data from shared drives has begun in areas with online SharePoint sites and a force migration plan has been agreed.

v. *Information Mapping*

The mapping of information across the organisation enables transparency on the data being held and the justification for its purpose. A review of the Records of Processing Activities and Information Asset Register will inform future data mapping under a new Information Governance structure.

3.5 INFORMATION SECURITY

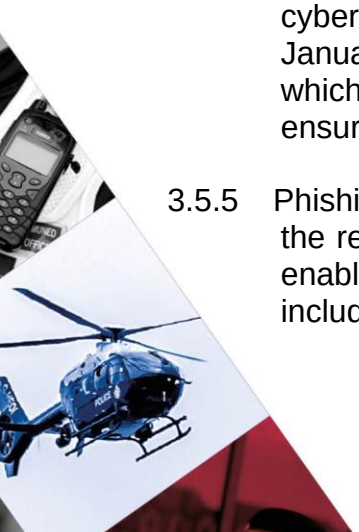
3.5.1 The Force Information Security Officer (FISO) delivers a comprehensive programme to audit and to test physical and cyber security. The programme is monitored through the Information Security Leadership Board and reported through force governance structures and is detailed at Annex 2.

3.5.2 The force has adopted the new Security Assessment Principles (SyAP) framework with the Police Digital Service and has aligned to the 110 controls. All controls were previously audited by Deloitte in 2020 as part of National Enabling Programme (NEP) and the force has seen an increase in its security posture score. In addition to this accreditation, the FISO aligns the force to various cyber frameworks including NIST 800-53, ISO27701, ISO27001, IASME as well as guidance from Audit Wales and the National Cyber Security Centre (NCSC).

3.5.3 National Enabling Programme (NEP) – the force has completed the full migration of all users and implemented full connectivity and full participation with the National Security Monitoring facility. The force is already using significant elements of the M365 capability to provide analytics, data warehousing and a number of other innovative applications to improve efficiency and effectiveness.

The force, as part of the NEP programme, utilises the National Monitoring Centre (NMC) as a Security Operations Centre (SOC). The force began utilising the NMC in May 2020. QRadar is the current Security Information and Event Management (SIEM) tool processing the alerts from log sources (firewalls, servers, endpoints etc), this will change to the Sentinel SIEM at the end of June 2023.

3.5.4 The force's cyber policies are reviewed annually and there is on-going delivery of cyber and data protection training to all staff – provided via the intranet site every January, June and October. The force undertakes an annual cyber tabletop exercise, which tests Business Continuity Plans and the Cyber Incident Response Plan to ensure they are fit for purpose.



3.5.5 Phishing continues to present a major threat to both individuals and businesses across the region as it is a common attack method to commit cyber-dependant and cyber-enabled crime, often at low cost to the criminal. The criminal intention for such attacks includes obtaining funds to initiate further cyber-attacks such as ransomware and to

gain unlawful access to computer networks and steal personal information from victims. The use of phishing is expected to remain as a high-level threat and is expected to continue to be delivered by email in the majority of incidents. The force undertakes half yearly phishing exercises to understand our susceptibility to such attacks.

3.5.6 Cyber incidents are an increasing threat nationally. Ransomware remains the common type of malware seen in the region and the threat has shifted from random attacks to more specific targets such as business, healthcare and the public sector. As such the National Strategic Assessment (NSA) outlines that ransomware has evolved from a serious criminal threat to a national security issue. Increasing reliance on digital technology solutions in the business, commercial as well as public sector, coupled with threats from hostile states and actors, increases the possibility and scale of cyber-attacks impacting at a national level. Over the last twelve months the force has not recorded any cyber incidents.

4. COLLABORATION

4.1 A baseline assessment of Gwent and South Wales Polices compliance with data protection obligations has been undertaken and enabled the joint DPO to assess compliance and areas for improvement, using the collaboration project to implement and align examples of best practice for each force. Processes have subsequently been consolidated into one process for both forces. The DPO has aligned data protection policies, so they are the same across both forces to enable best practice as well as alignment for collaborative units.

The DPO advises the Senior Information Risk Owners (SIROs) of both forces over many common areas, as a result of the system and service alignment that has been developed in collaboration.

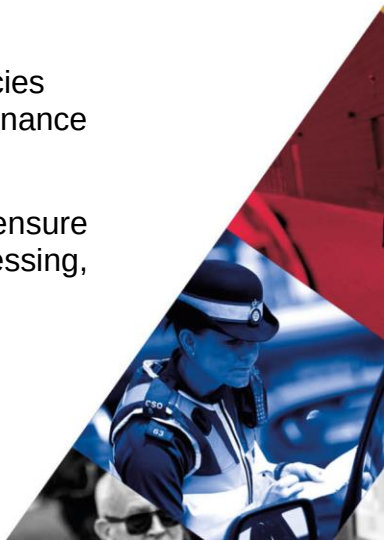
The introduction of the National Enabling Programme provides M365 SharePoint and a corporate document structure, which is being implemented in line with the National Police Chiefs Council (NPCC) guidance and will enable both forces to share documentation in a more accessible manner and improve the efficiency of our collaborative teams.

5. NEXT STEPS

5.1 The force will continue to report its improvement plans and overall performance through the Information Assurance Board.

5.2 The Joint DPO will complete the alignment of data protection policies and review of the resource and structure of the Information Governance team.

5.3 Complete the Information Sharing Agreements to ensure compliance, monitoring and maintenance of the Records of Processing, Information Asset Register and Information Risk Register.



5.4 Appropriate data governance will be provided to support the full rollout of M365.

6. FINANCIAL CONSIDERATIONS

There are no financial considerations in this report.

7. PERSONNEL CONSIDERATIONS

Training and support are provided to staff to ensure they are able to meet the obligations of their role.

8. LEGAL IMPLICATIONS

There are no legal implications at this stage.

9. EQUALITIES & HUMAN RIGHTS CONSIDERATIONS

This project/proposal has been considered against the general duty to promote equality, as stipulated under the Single Equality Scheme and has been assessed not to discriminate against any particular group.

In preparing this report, consideration has been given to requirements of the Articles contained in the European Convention on Human Rights and the Human Rights Act 1998.

10. RISK

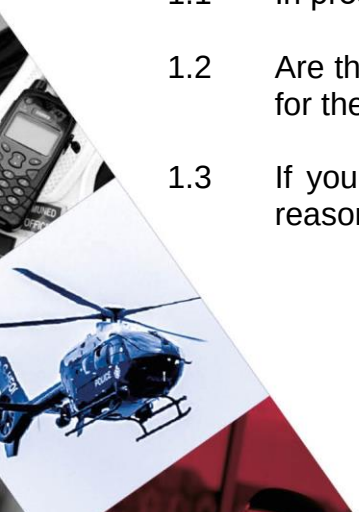
None.

11. PUBLIC INTEREST

1.1 In producing this report, has consideration been given to 'public confidence'? **Yes**

1.2 Are the contents of this report, observations and appendices necessary and suitable for the public domain? **Yes**

1.3 If you consider this report to be exempt from the public domain, please state the reasons: **N/A**



12. REPORT AUTHORS

Natasha Gilbert, Head of Information Services
Louise Voisey, Joint Data Protection Officer
Kathy Buckley, Force Information Security Officer.

13. LEAD CHIEF OFFICER

Nigel Stephens; Assistant Chief Officer – Resources

14. ANNEXES

Annex 1 - Subject Access and Freedom of Information
Annex 2 - Information Security Reporting Framework

15. CHIEF OFFICER APPROVAL

15.1 I confirm this report has been discussed and approved at a formal Chief Officers' meeting.

15.2 I confirm this report is suitable for the public domain

Signature: Nigel Stephens **Date:** 31/05/2023