ACCOUNTABILITY BOARD

Meeting to be held on 18 June 2024

Data Protection Office Annual Report 2023/24

Contact for further information: Ian Dickinson, 01772 533587, Office of the Police and Crime Commissioner, ian.dickinson@lancashire-pcc.gov.uk

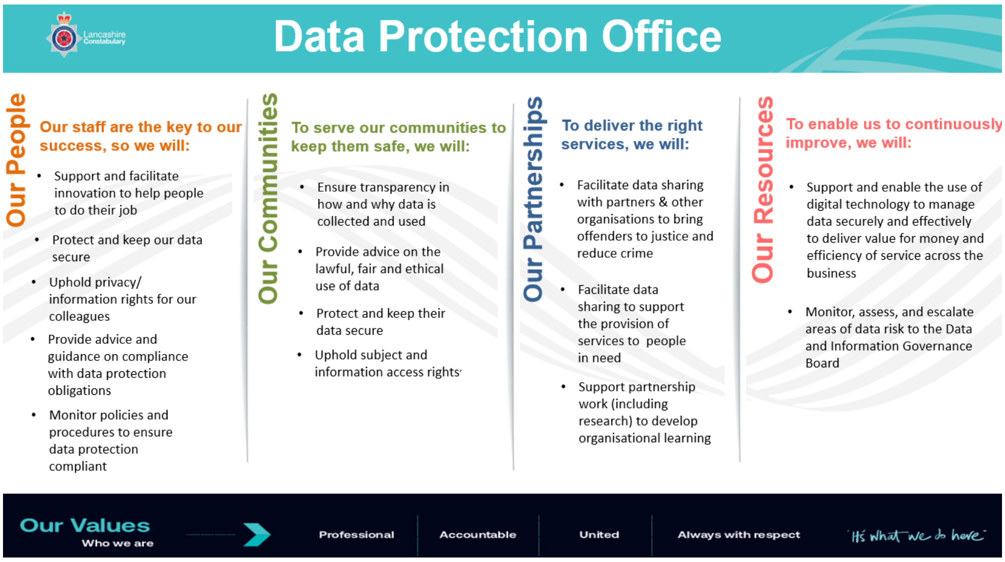
Executive Summary The purpose of this report is to provide the Commissioner with an overview of the Constabulary's performance and progress in relation to information governance during 2023/24.
Recommendation The Commissioner is requested to review the report and make comments as appropriate.

1.0 Introduction

1.1 The Data Protection Office undertakes the following information governance functions:

- Information security
- Records management – including review, retention & deletion and M365
- Information sharing
- Compliance – including data law, data sharing/ data protection audit
- Information access – subject access/ FOIA

1.2 The way in which the Office supports the Strategic Vison and plan can be seen below:



Data Protection Office

Our People

Our staff are the key to our success, so we will:

- Support and facilitate innovation to help people to do their job
- Protect and keep our data secure
- Uphold privacy/ information rights for our colleagues
- Provide advice and guidance on compliance with data protection obligations
- Monitor policies and procedures to ensure data protection compliant

Our Communities

To serve our communities to keep them safe, we will:

- Ensure transparency in how and why data is collected and used
- Provide advice on the lawful, fair and ethical use of data
- Protect and keep their data secure
- Uphold subject and information access rights

Our Partnerships

To deliver the right services, we will:

- Facilitate data sharing with partners & other organisations to bring offenders to justice and reduce crime
- Facilitate data sharing to support the provision of services to people in need
- Support partnership work (including research) to develop organisational learning

Our Resources

To enable us to continuously improve, we will:

- Support and enable the use of digital technology to manage data securely and effectively to deliver value for money and efficiency of service across the business
- Monitor, assess, and escalate areas of data risk to the Data and Information Governance Board

Our Values
Who we are

Professional | Accountable | United | Always with respect

It's what we do here

1.3 In summary, during the course of 2023/24 the Department has continued to make good progress against a number of its objectives and annual priorities. This has included maintaining good performance with regards to the statutory timescales for compliance with Freedom of Information Act 2000 requests and subject access requests for personal data under the Data Protection Act 2018/ UK GDPR, adoption of and delivery of a data protection audit plan, development of a M365 knowledge Centre, improvements to the force's information security assessment rating, implementation of new security incident reporting process, progress against records management priorities and engagement at NPCC level to help influence national workstreams.

2.0 Resources

2.1 The Data Protection Office is comprised of 22.2 FTE posts.

2.2 During the course of 2023/ 24 successful recruitment enabled a number of vacancies to be filled, following vacancies across the department being carried for a prolonged period. In this time individuals within the department have continued to develop and received formal training relevant to their role, as per the Department's training plan. The Department is presently carrying two vacancies for the roles of 'M365 Records Management and Security Advisor' and Information Access Admin Assistant. However, proposals are being made to disestablish these vacant roles in order to utilise the resources to better help manage existing and predicted demands. This will include the establishment of a data protection advisor role that will focus in particular on the ethical use of data.

3.0 Governance

3.1 In 2023 the Constabulary approved a new Information and Data Management Strategy. The Strategy emphasises the priority to support a data driven culture which maximises the value of data through technology in a manner that is lawful, ethical, and secure.

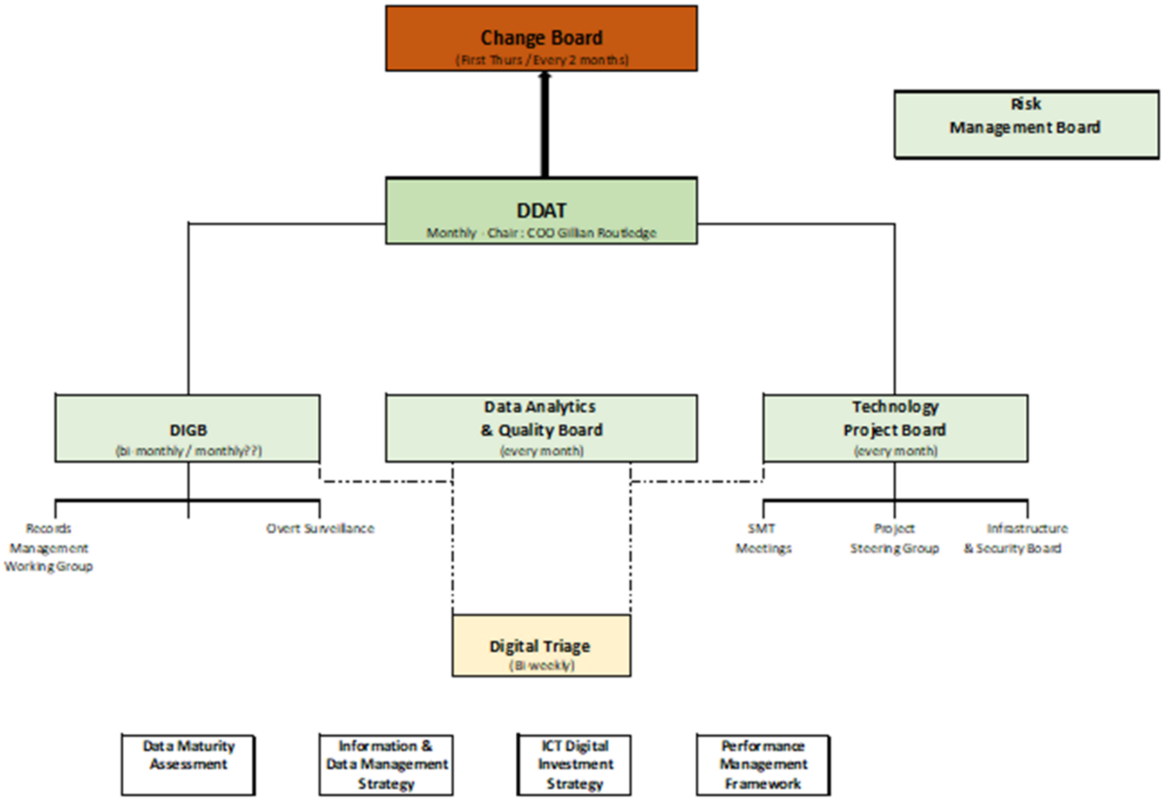
3.2 Reports from the Data Protection Office were presented to the Data and Information Governance Board, chaired by the Chief Operating Officer, on a quarterly basis.

3.3 During the course of 2023, all the Department's policies and procedures were reviewed and revised where appropriate.

3.4 During 2023/ 24 two data maturity assessments of Lancashire Constabulary were undertaken (PDS/ Simpsons Associates) and the report 'Protecting from Within': A review commissioned by the Police Service of Northern Ireland (PSNI) and the Northern Ireland Policing Board into the PSNI data breach of the 8th August 2023 was published. The latter report addressed and made recommendations relation to data governance functions.

3.5 Whilst the Constabulary was generally well positioned, a review of these reports is informing the development of an Information and Data Management Strategy Delivery Plan; the findings were also acknowledged when establishing the new data governance framework within the force, developed with the Head of ICT and Head of Corporate Services.

3.6 The new arrangements seek to improve corporate oversight and control the use of data and new technologies, considering business requirements and ensuring that due diligence is completed. The new model (below) will seek to ensure that information asset (data) owners are fully aware of their role and seeks to embed accountability.

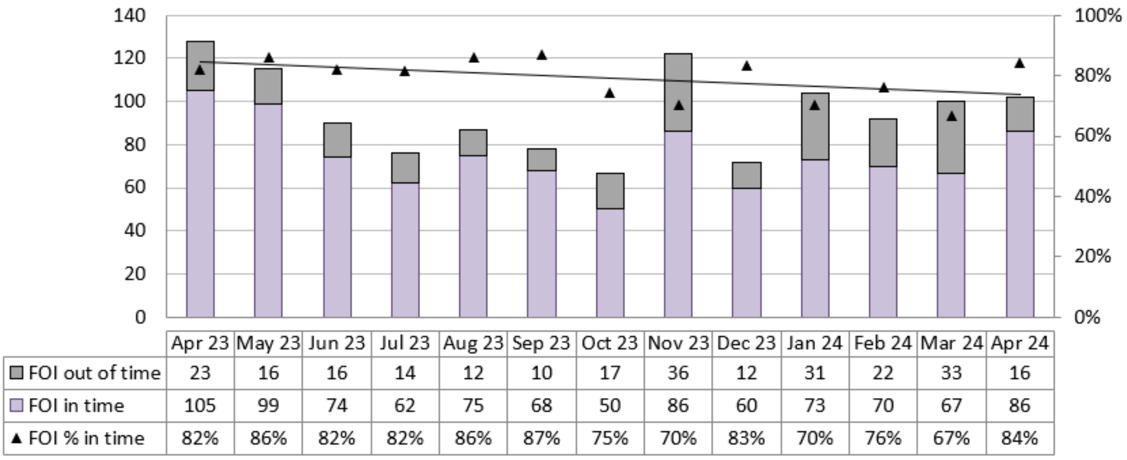

Change Board
(First Thurs / Every 2 months)
Risk Management Board
DDAT
Monthly · Chair : COO Gillian Routledge
DIGB
(bi-monthly / monthly??)
Data Analytics & Quality Board
(every month)
Technology Project Board
(every month)
Records Management Working Group
Overt Surveillance
SMT Meetings
Project Steering Group
Infrastructure & Security Board
Digital Triage
(Bi-weekly)
Data Maturity Assessment
Information & Data Management Strategy
ICT Digital Investment Strategy
Performance Management Framework

4. FOIA Compliance

4.1 The Freedom of Information Act 2000 (FOIA) sets a statutory deadline of 20 working days for public authorities to respond to requests for information. The ICO expects that public authorities meet this requirement for 90% of the requests it receives.

4.2 The chart below highlights performance against statutory timescales over the past 13 months.

Completed FoI Requests - numbers completed in / out of timescales and percentage completed in time



	Apr 23	May 23	Jun 23	Jul 23	Aug 23	Sep 23	Oct 23	Nov 23	Dec 23	Jan 24	Feb 24	Mar 24	Apr 24
▨ FOI out of time	23	16	16	14	12	10	17	36	12	31	22	33	16
□ FOI in time	105	99	74	62	75	68	50	86	60	73	70	67	86
▲ FOI % in time	82%	86%	82%	82%	86%	87%	75%	70%	83%	70%	76%	67%	84%

4.3 Over the course of the year performance remained consistent. The compliance rate dipped in October and November but returned to over 80% in December. Whilst the performance is below ICO expectations (90%) it compares well with most forces.

4.4 It should be noted that when compared with the number of requests in 2022 (1098), 2023 saw an increase of 18% with 1320 requests being received.

4.5 There were 38 internal reviews received in 2023 compared to 19 in 2022. In four of these cases following the review being undertaken some further information was provided.

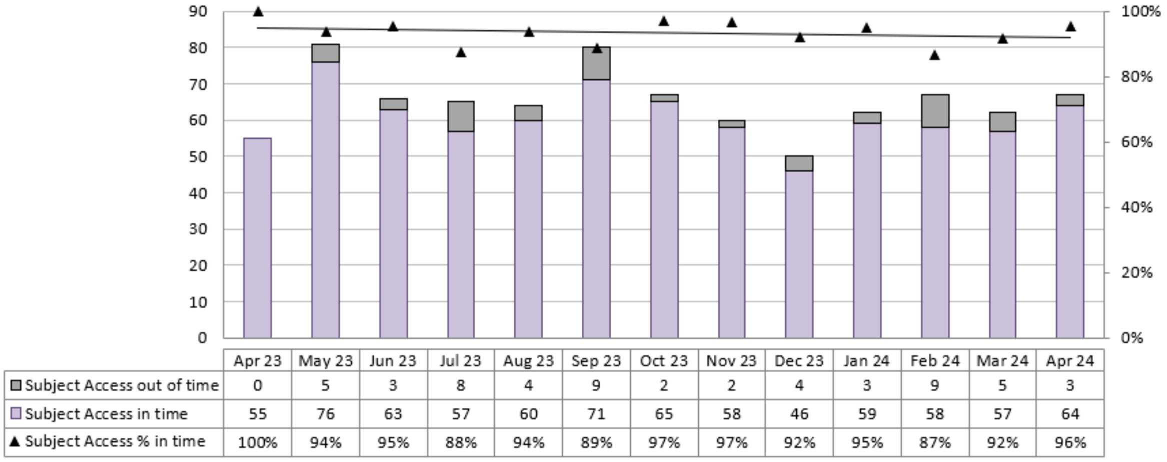
4.6 There were five complaints made to the ICO with four decision notices (DN) finding in favour of the Constabulary. One ICO DN is subject to challenge at the First Tier Tribunal. One complaint was upheld by the ICO and the DN required the Constabulary to disclose two further documents.

4.7 The FOIA requires that public authorities proactively publish information as part of their publication scheme. During 2023/24 a review of the content of the Publication Scheme has been undertaken, gaps identified, and work is on-going to update/ fill the gaps. It is expected that this work will be completed in the first quarter of 2024/25.

5. Subject Access Compliance

5.1 Data protection legislation gives individuals various rights, one of which is to receive confirmation as to whether their data is held by an organisation and if so to receive a copy, within a calendar month of the request being received. The chart below highlights performance against statutory timescales over the past 13 months.

Completed Subject Access Requests - numbers completed in / out of timescales and percentage completed in time



	Apr 23	May 23	Jun 23	Jul 23	Aug 23	Sep 23	Oct 23	Nov 23	Dec 23	Jan 24	Feb 24	Mar 24	Apr 24
■ Subject Access out of time	0	5	3	8	4	9	2	2	4	3	9	5	3
□ Subject Access in time	55	76	63	57	60	71	65	58	46	59	58	57	64
▲ Subject Access % in time	100%	94%	95%	88%	94%	89%	97%	97%	92%	95%	87%	92%	96%

5.2 Compliance rates with SAR's over 2023 met the ICO's 90% expectation, despite the highest volume of SARs ever received by the Constabulary. 811 requests were received in 2023, compared to 684 in 2022 (19% increase). Again, Lancashire's performance compares favourably against most forces.

5.3 There have been 27 'internal reviews' considered where the applicant has expressed dissatisfaction with their response. One complaint to the ICO was made, whereby the ICO found that Lancashire Constabulary had complied with its obligations and no further action was required.

6. Information Access (FOIA/ Subject Access) Demand/ Risk

6.1 The increase in demand for FOIA/ subject access requests is one which has been mirrored across the police service. Lancashire has maintained strong performance and has been able to absorb the increase in demand to date. This is as a result of a mature team that has developed its knowledge over the past few years and following the introduction of a new case management system two years ago which delivered some efficiencies. However, the capacity of the team is now stretched. The Head of Data Protection has been engaging at a national level in order to identify what, if any, opportunities exist to introduce automation within force processes and also on the system/ user needs within the work to identify enhanced redaction tools. And the Head of Data protection is also working on the development of an Open Data Strategy and the proactive publication of data sets.

6.2 In the meantime, a review of the department and proposals to make minor changes to the Department structure will seek to provide some additional resilience by the establishment of an additional 0.5 FTE Information Access Officer post.

6.3 The ICO has highlighted in 2024 the need for public authority leaders to take transparency seriously and more stringent enforcement action may be taken against some police forces.

7. Data Protection by Design (DPbD) and Data Protection Impact Assessments (DPIA)

7.1 Data protection legislation is a core date protection requirement introduced by the General Data Protection Regulation and a legal requirement. It requires an approach that implements appropriate technical and organisational measures such as pseudonymisation with a view to implementing data protection principles such as data minimisation and facilitating subject rights.

7.2 In addition, when undertaking processing where there is potentially a high risk to the privacy rights of the individuals whose data is to be processed, then a DPIA is required.

7.3 When considering new systems or processes, a screening process is undertaken which highlights whether a DPIA is required or in the case of the processing of personal data which does not require a DPIA then a DPbD assessment.

7.4 An audit of the Constabulary's completed DPIAs was included on the 2023-2024 Department's data protection audit plan. The aim of the audit included ensuring completed DPIAs are still accurate and assessing whether the DPIAs have been updated where necessary.

7.5 Of the 21 live DPIAs, five had been reviewed or completed within the past year. Of the remaining 16 DPIAs, one had been reviewed in 2023 and 15 were about to be reviewed in 2024.

8. Data/ Information Sharing

8.1 The Data Protection Office maintains an information sharing register. The department has continued to support the establishment of new and the review of existing information sharing agreements.

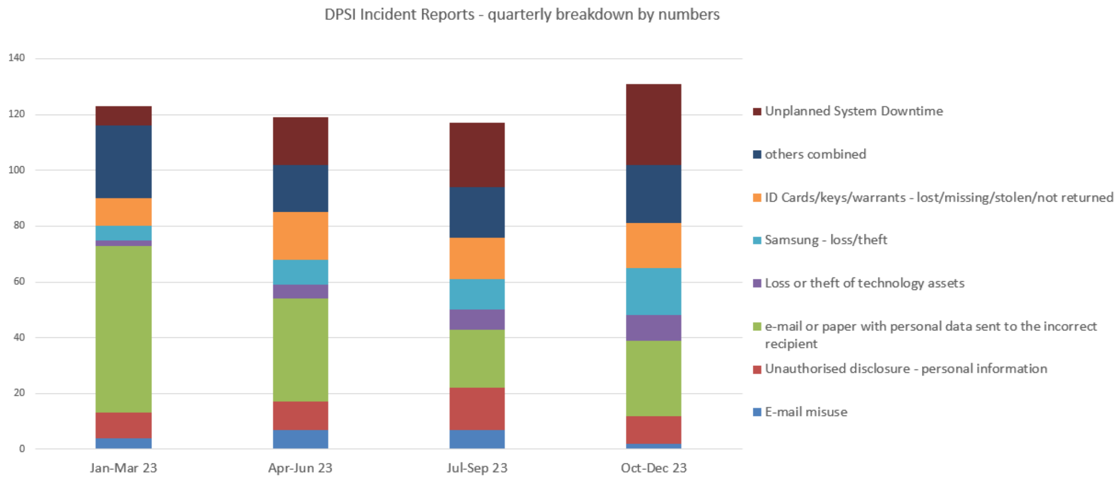
8.2 Of particular note is the engagement relating the Family Hubs Information Service (FHISS); this project aims to deliver a shared digital solution that will provide a holistic picture of families enabling practitioners to provide better outcomes for children and their families. It is a Lancashire County Council hosted system which seeks to centralise relevant data from the council, police, and health. It aligns with the government data strategy and ambitions of the National Police Chief's Council (NPCC). Work is now ongoing to identify data sets that are required for the purpose of the FHISS, and an Information Sharing Agreement is being written to reflect the agreed data sets, lawful basis, and the security of the data.

8.3 Representatives from the Data Protection Office sit on the NPCC Data Sharing Quality Assurance Panel and the NPCC Data Sharing Steering Group.

8.4 During 2023, the Information Sharing and Disclosure Policy, along with relevant guidance documents were reviewed and revised. These will be highlighted within the Communications to be published during 2024.

9. Data Protection and Security Incidents

9.1 During 2023 490 security incidents were reported to the Data Protection Office. The nature of these incidents is summarised below:



	January - March	April - June	July - September	October – December 2023	2023 Total
E-mail misuse	4	7	7	2	**20**
Unauthorised disclosure - personal information	9	10	15	10	**44**
e-mail or paper with personal data sent to the incorrect recipient	60	37	21	27	**145**
Loss or theft of technology assets	2	5	7	9	**23**
Samsung - loss/theft	5	9	11	17	**42**
ID Cards/keys/warrants - lost/missing/stolen/not returned	10	17	15	16	**58**
Others combined	26	17	18	21	**82**
Unplanned System Downtime	7	17	23	29	**76**
Total	**123**	**119**	**117**	**131**	
	Total 2023 – 490 Incidents				

9.2 The reporting incident procedure is well established within the Constabulary. All incidents are assessed, advice provided, and remediation steps taken where appropriate. It should be noted that not all incidents will result in a personal data breach.

9.3 With regard to ‘email misuse’ this is captured using the Data Loss Prevention (DLP) tools within M365 Purview Compliance centre. This rule identifies emails or documents marked official- sensitive being sent to external non-secure personal email addresses. These incidents relate to staff sending information to staff sending work to their private emails. When identified staff are spoken to by the Data Protection Office and given advice to prevent repeated incidents. ‘Others combined’ relates to a security or data protection incident that does not fit into the other categories. It captures reports of malware being detected or unusual emails being reported as well as the theft of paper documents such as paper notebooks. Most of these incidents relate to malware being blocked or reports of suspicious emails.

9.4 There has been one personal data breach reported to the Information Commissioner (ICO). A video was published on the social media platform Tik Tok as part of Operation Brightsparx which sought to reduce anti-social behaviour in the run up to Bonfire Night. The video included un-redacted footage of a 16-year-old boy at a custody desk following arrest. This matter remains on-going.

9.5 The ICO also wrote to the Constabulary seeking information regarding the sharing of information to the Disclosure and Barring Service, from Connect via the PLX system, in order to determine whether a formal investigation was required. This followed the identification of possible issues resulting in the processing of inaccurate information by the DBS. The matter had not been referred to the ICO due to the assessment that this presented a low risk to any individuals who might have been affected. However, the issue has been subject to national consideration and a detailed submission regarding the matter has been provided to the ICO.

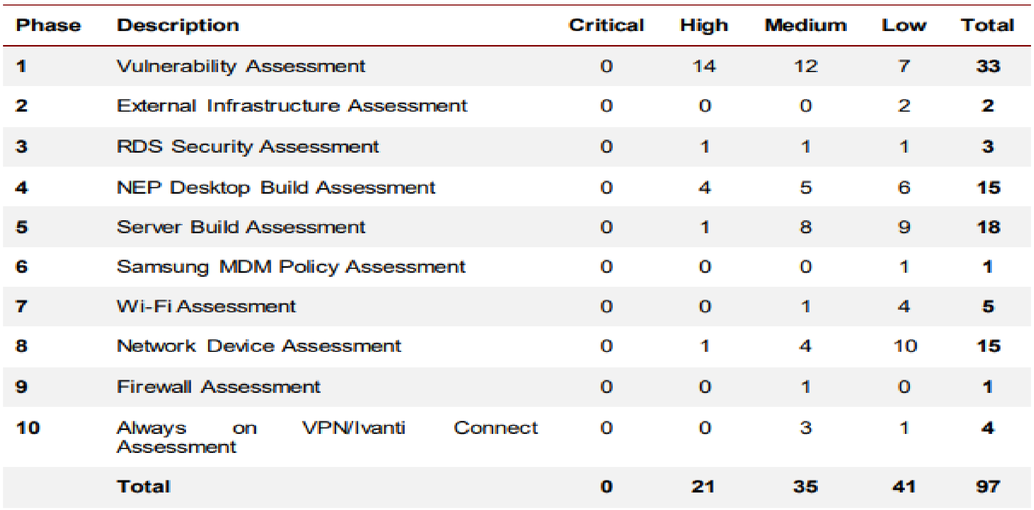
9.6 The Constabulary also provided detailed information in relation to the background and context relating to the decision to disclose in information relating to the missing person, Nicola Bulley. This followed widespread criticism of the disclosure of information during the missing person inquiry. No formal action was taken by the ICO.

10. Information Security

10.1 The Information Security Team within the Data Protection Office work closely with colleagues in ICT and engage with the National Management Centre, regarding cyber threats.

10.2 The Constabulary has maintained accreditation for key national systems; it maintains its Public Service Network in Policing (PSNP) compliance with the successful completion of the Security Assessment for Policing (SyAP). The PSNP compliance will be used as the gateway to allow us to access national systems. During 2023 the Constabulary improved its maturity rating over and above the national baseline and improvements against the SyAP are improving.

10.3 The Constabulary's 2023 annual ITHC was completed the 15th June to 4th July 2023. This report highlighted the following vulnerabilities.



Phase	Description	Critical	High	Medium	Low	Total
1	Vulnerability Assessment	0	14	12	7	**33**
2	External Infrastructure Assessment	0	0	0	2	**2**
3	RDS Security Assessment	0	1	1	1	**3**
4	NEP Desktop Build Assessment	0	4	5	6	**15**
5	Server Build Assessment	0	1	8	9	**18**
6	Samsung MDM Policy Assessment	0	0	0	1	**1**
7	Wi-Fi Assessment	0	0	1	4	**5**
8	Network Device Assessment	0	1	4	10	**15**
9	Firewall Assessment	0	0	1	0	**1**
10	Always on VPN/Ivanti Connect Assessment	0	0	3	1	**4**
	Total	**0**	**21**	**35**	**41**	**97**

All Highs (21) have been corrected and are either complete or in the process of deployment which can take time due the size and complexity of the IT estate.

10.4 Phishing attacks across all sectors and government bodies increased in 2023. Lancashire was no different and evidenced by:

- A sharp rise in QR codes embedded within the body of emails
- Unsophisticated campaign from Gmail domains of spear phishing emails trying to open up communication with the named recipient
- Artificial Intelligence is vastly improving the quality of email crafting. Better grammar, more specific content aimed at users or industry
- Clear rise in the use of reconnaissance from LinkedIn to improve spear phishing

10.5 During 2023, a programme of education via comms and phishing simulations saw user awareness improve. To date 79% of users across the Constabulary have completed simulation. As a force, we have remained under the predicted compromise rate and continue to improve, with continued simulations and further training and education planned.

10.6 2023 saw a number of cyber-attacks on third parties who host police data. To help mitigate against this risk, the force has implemented Risk Ledger, a supply chain risk platform that enables compliance with security requirements such as ISO27001 to be monitored. The use of the tool is increasing across policing. It will enable the Information Security Team to conduct more efficient and timely risk assessments of new and existing suppliers. This is particularly important as the cyber threat has increased and third-party suppliers that hold police data may be vulnerable if they do not maintain appropriate cyber defences. Risk Ledger is now being used for any new systems and the next step is to review and onboard current suppliers in use before this implementation.

11. Audit

11.1 During 2023/24 the Department was able to establish and deliver against a data protection audit plan.

11.2 The Chief Constable as Controller is accountable for compliance with the principles of data protection legislation. Monitoring of data protection compliance falls within the statutory duties of the Data Protection Officer. The Audit process is designed to check compliance with legal, regulatory, contractual and procedural obligations, including: DPA, GDPR, Computer Misuse Act 1990, Human Rights Act 1998, Freedom of Information Act 2000, Regulation of Investigatory Powers Act 2000, Codes of Connection (CoCos), ISO 27001/ 27701 relating to information security and national, force standards, polices and good practice. The audit plan includes transactional audits of systems, such as the Police National Computer (PNC), Police National Database (PND) and ANPR, amongst others, so as to ensure that those that access data do so have a legitimate purpose to access the data, and to detect and deter unauthorised access. The plan also included compliance audits which addressed broader data protection responsibilities.

12. Records Management

12.1 Good progress continues to be made to address the excessive retention of records across numerous systems, as a consequence of legacy systems issues. A Records Management Working Group, with representatives from across all business areas, reports into the Data and Information Governance Board, and a bi-annual report is presented to the Chief Officer Team.

12.2 Deletion requests: The Review, Retention and Deletion (RRD) Team process 'deletion requests'. During 2023 33 requests were received for Lancashire information held on the PNC, and 16 requests were received for the deletion of information from local records.

12.3 Custody Images: National Custody Image and Strategic and Facial Matching Programme commenced in October 2023 with the Home Office investing £500K over 2 years to establish a Custody Imaging and Strategic Facial Matching Programme. A retention policy similar to that governing biometrics is being explored. The vison of the programme is to support policing in visibly and proactively managing high quality custody images in accordance with law to ensure public confidence, and to support policing in making the most effective use of facial recognition for the prevention and detection of crime and supporting the vulnerable.

12.4 The Records Manager is the Lancashire SPOC and has responded to a questionnaire circulated to all forces as part of the initial landscape review. During 2024 this programme of will continue.

12.5 In the meantime, the RRD team commenced a process of reviewing custody images triggered by the deletion of biometrics due to a recent 'No Further action (NFA)' outcome. This has now been established as 'business as usual' and the volumes reviewed are detailed in the table below:

Date	Total Reviewed	Deleted	Retained
Nov-23	166	153	14
Dec-23	104	95	9
Jan-24	98	93	5
Feb-24	126	115	11
Mar-24	56	54	2

12.6 The Programme Lead subsequently approached the Records Manager to highlight within the work programme, the approach recently adopted within Lancashire.

12.7 Unofficial Record Stores: Following contact by the Head of CJ regarding a number of unofficial file/document/exhibit/property stores in various locations within East BCU (termed 'Pop-up Stores'), the Records Management Team have been working with CJ colleagues and colleagues in East Division to address a long-standing issue that has accumulated over a lengthy period of time.

12.8 The RRD officers have been working with the Long-Term Storage officers in the BCU to systematically review NFA crime files located at Greenbank, with MoPI 3 offence files will be destroyed in situ. The remaining files have been transferred to the storage facility at Accrington for recording purposes and will be subject to review by RRD officers as necessary. An individual(s) with a PPU background will be appointed to conduct a dip sampling exercise of the child protection files and liaison will be undertaken with the Records Manager to determine the appropriate action. Findings regarding exhibits and property will be shared with two nominated Chief Inspectors who will ensure any necessary actions are undertaken regarding storage or disposal.

12.9 It is probable that similar issues will exist in the other two BCUs and the intention is to extend the and carry out a similar exercise in 2024 within those areas. These actions will have a positive impact on the drive to move to a paperless regime, reduce compliance risk and improve accountability.

12.10 Legacy Systems: Sleuth is comprised of a number of a legacy systems, which some parts of the Force still access. On 30 October 2023 Sleuth accounts for most officers and staff were removed (select groups of staff will retain accounts until outstanding issues are resolved) with only limited access being provided to small data set of records that had not been back record converted in to CONNECT. Work is on-going to address this issue with the Head of ICT and the relevant Information Asset Owners.

12.11 Operation Papercut: A project of work commenced in 2023 to reduce the number of paper records held by the Force, via digitisation or destruction. A driver for this piece of work is the future re-development of the HQ site. And therefore, HQ departments have been prioritised. Engagement with HQ departments was undertaken, and the findings assessed, with each department being rated. Progress continues to be made across departments and where the more difficult issues have been identified, engagement with departments is on-going in order to identify the most practical solutions and identify potential costs.

12.12 Code of Practice for Police Information & Records Management and Archiving Authorised Professional Practice (APP): The Code of Practice for Police Information and Records Management replaced the previous Code of Practice for Management of Police Information (2005) in July last year. It covers corporate record keeping and is more reflective of the modern data protection landscape. The new Code is supported by APP (Information Management, Management of Police Information). A gap analysis has been undertaken highlighting the areas requiring development to achieve compliance. This will be developed into an action plan and form part of the Information and Data Management Strategy delivery Plan.

13 M365 Team

13.1 M365 provides a complete software as a service solution, with apps and cloud-based services. It provides tools which enable records to be more effectively managed. The M365 Records Management and Security Team have undertaken comprehensive audits of the current Teams and the SharePoint Online landscape within the Force to ensure records are accurate and Teams/SharePoint Sites which are not being used are removed if no longer wanted.

13.2 A M365 Knowledge Hub comprising of a comprehensive collection of 'How To' guides and videos has been developed and published to provide staff and officers with guidance on how to use all the most common features of Teams, also covering aspects of Teams, OneDrive and SharePoint Online that staff and officers may be unaware of that could be beneficial. The videos included within the M365 Knowledge Hub have also been added to Kallidus so individuals can complete and evidence the learning that they have undertaken, or managers could choose to assign any of the learning packages to their staff if they think it will be beneficial.

13.3 As part of Operation Papercut, the M365 Team Supervisor has attended meetings alongside the Records Manager with all Heads of Departments to discuss Operation Papercut and understand what each department is currently holding in paper records, then provide recommendations on how those records and the processes that create the records could be reduced and/or digitalised utilising M365 Cloud storage solutions.

13.4 Migration to SharePoint Online: Microsoft support for SharePoint 2016 expires in 2026. Work to migrate commenced in 2023. Migration is split in to three main phases, with multiple steps within each stage which need completing before a department can move onto the next stage. These main stages are the Discover Phase, Prepare Phase and Migrate Phase.

13.5 Progress as of March 2024, can be summarised below: The departments are listed in order of date approached, with the first department beginning their migration journey in January 2023 and the BCU's commencing their engagement in January 2024.

	Discover			**Prepare**			**Migrate**				
Department	Engaged	Overview Delivered	Plan Approved	Mapping Data	Implementation Plan Sent to Department	Implementation Plan Approved	Build & Pre-Check	Migration Scheduled	Migration Complete	Final Sign off	Department Migrated
ICT	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢			
Estates	🟨	🟨	🟨	🟨	🟨						
Corporate Development	🟧	🟧									
Scientific Support	🟨	🟨	🟨	🟨							
Criminal Justice	🟨	🟨	🟨	🟨	🟨						
HR	🟧	🟧									
Legal	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Organisational Development	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
PPU	🟧	🟧									
Chief Officers	🟨	🟨	🟨	🟨							
Learning & Development	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Data Protection Office	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Finance	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢			

Media & Engagement	🟧	🟧									
Contact Management	🟨	🟨	🟨	🟨	🟨						
Operations	🟧	🟧									
Intel & Crime Support	🟧	🟧									
Fleet	🟩	🟩	🟩	🟩	🟩	🟩	🟩				
PSD	🟧	🟧									
CTB	🟧	🟧									
FMIT	🟧	🟧									
ASB	🟧	🟧									
East BCU	🟧										
South BCU	🟧										
West BCU	🟧										

Key:

🟧 In Discovery Phase	🟨 In Prepare Phase	🟩 In Migration Phase	Migration Complete

13.6 Progress remains on track; however, the M365 Team are working closely with departments to try to ensure each department continues to progress however some departments are progressing quicker than others.

13.7 A large aspect of this project involves departments reviewing their current data stored in on-premises storage solutions and actively weeding it to remove old, over-retained or duplicated files. This ensures that when a department is ready to begin migrating files into the new Cloud storage solutions that only the data that is relevant and needed is migrated across. As departments are progressing with their migration journey, it is expected that the number of files remaining in the on-premises storage solutions will decrease as files are being reviewed and deleted. The work undertaken to data has seen a reduction of over two million files since the migration project began.

14. Training

14.1 Training is provided to all new staff at induction via a face-to-face input and an on-line module within Kallidus. Training has been provided upon request by the department in relation to security incidents, DPIA's, SharePoint, etc.

14.2 Whilst mandatory data protection/ information management training has been provided in the past, it has been agreed to issue mandatory training during 2024/ 25.

15. Horizon Scanning & Priorities for 2024/ 25

15.1 Data, utilising new technologies, will continue to be the key driver in delivering the Constabulary's vison and strategy. In maximising digital technologies, data must be accurate, and processed lawfully, fairly, ethically, transparently, and securely.

15.2 The development of the Information and Data Management Strategy Delivery Plan will provide the focus through which improvements to data accountability, legacy records management issues, and the strengthening of cyber and information security, can be monitored. This will include the further development of the cyber incident Response Plan, strengthening third party supplier management, and the development of data literacy/ awareness. Training will be delivered to Information Asset (Data) owners in 2024.

15.2 The Data Protection and Digital Information Bill will likely receive royal ascent in the summer of 2024. The final content is still under debate. Work will be required to understand the full impact of the changes and their impact for the department and the Constabulary.

15.3 Presently, the UK Government do not intend to introduce regulation to govern the use of Artificial Intelligence (AI) and the response to AI White Paper highlights how the ICO will work closely with other regulators. However, this is an evolving area with legislation emerging across other countries and continents. The use of Artificial Intelligence (AI) within digital tools will continue to increase and work will be required to identify and incorporate AI compliance obligations within the existing privacy and data governance frameworks. This will include but not be limited to the development of a data ethics framework. In recognition of this, as highlighted earlier, it is intended to establish a data protection advisor post which will have a particular focus on ethics and innovation.

15.3 The ICO has called upon senior leaders to take transparency seriously and highlighted that a firmer approach may be undertaken if enforcement action is considered. Further work will be undertaken to explore how best to address the growth in demand for FOIA/ subject access requests, via new technologies and a pro-active approach to data publication.