London Borough of Enfield

NOTE TO REPORT AUTHORS AND OTHERS: Until this report is published, even if it is ultimately to be considered in Part 1, it should not be circulated beyond the Cabinet (excepting officers writing and reviewing the paper through this process) or sent externally, and its contents should be treated as confidential.

Report Title:	**Annual Report of the Information and Data Governance Board**
Report to:	**General Purposes Committee**
Date of Meeting:	**16th March 2023**
Cabinet Member:	**Tim Leaver**
Directors:	**Fay Hammond and Paul Neville**
Report Author:	**Martin Sanders martin.sanders@enfield.gov.uk**
Ward(s) affected:	
Classification:	Part I Public
Reason for exemption	No applicable

Purpose of Report

1. To recognise that the governance arrangements remain broadly the same and are working well.
2. To recognise some of key changes introduced successfully since the last report.
    a. The improvement in achieving over 98% compliance in completing mandatory training and introduction of Data Governance reporting into the board.
    b. The high standard data retention schedule now covering over 450 sets of data

3. To highlight the plans of the board for 2023/24.

Recommendations

I.	Agree the inclusion of Covid Inquiry Information and Data Governance to be monitored through the board until concluded.
II.	Approve the outcomes of this annual report.
III.	To note the achievement of mandatory training compliance.
IV.	To note the achievement of high standard data retention schedule.
V.	Approve the plan for 2023/24
VI.	To note the risks

Background and Options

4. The Information and Data Governance Board scrutinises the council's use of information to ensure it remains compliant with statutory and council standards. The board is chaired by the Head of Service Management and Governance and has required attendance from all council departments, in addition to standing membership from Information and Data Governance, Digital and Corporate Security, Learning and Development, Complaints and Data Protection.

   The Board meets monthly and provides reports to the Assurance Board.

   Membership of the Board is comprised of Head of Service Management and Governance (Chair), Information and Data Governance Manager (Deputy Chair), Head of Corporate & Cyber Security, Head of Audit and Risk, Data Protection Officer, Business Development Managers for each Department, Digital Security representatives and Complaints and Information Manager. The council has also added the Director of Public Health to the board as part of overviewing the information and data required for the Covid inquiry.

   In 2022/23 the board introduced further reporting standards, so that reporting on the following streams was provided on monthly or quarterly basis.

   - Cyber Security
   - Data Protection
   - Data Quality and Governance
   - Covid Enquiry
   - Information and Data Governance and Compliance
   - Learning and Development
   - Freedom of Information, Complaints, Subject Access Requests and Members Enquiries

   The board also introduced an annual plan to ensure a rolling review of standards, risks, policies, processes and compliance to ensure that these are maintained, improved, approved and then publicised throughout the organisation.

5. The impact of the pandemic has seen a change in working styles in the

council which is now established as the norm. The Smart Working Policy provides support for staff working flexibly, working both in the office and from home. At the height of the pandemic around 80% to 90% of staff were remotely, and while more staff have returned to the office, each day there are still more staff working remotely than in the office.

The additional challenges this introduced have been addressed and are now embedded in the council's ways of working, technology and policies and supported by increased education and awareness.

These included:

- Increased levels of cyber threats and attacks
- Protection of information and data when working at home
- Reduced on site staffing and working in locations where they may not be familiar with other people
- Accelerated move from using paper to electronic information
- Increased use of video and social media tools such as Zoom, WhatsApp
- Holding public meetings online
- Frequency of change and guidance regarding where to work
- Working from abroad

Actions to address these challenges that have been monitored at the Information and Data Governance Board, have included the following.

- Increased training and education, including mandatory reporting and undertaking of Cyber Security, Data Protection and Information and Data Governance Training which are now built into Personal Development Reviews
- Improved Cyber Security technology and reporting of incidents
- Undertaking simulations of events such as Cyber-attacks, Security Breaches and monitoring compliance with Information and Data Governance policy and processes
- Specific campaigns raising awareness of changes, risks and individual responsibility regarding Information and Data Governance
- Changed processes for requesting and monitoring access for working from abroad

6. Key Improvements and Changes made since the last report

7. Mandatory Training

   Mandatory Training for Cyber Security and Data Protection parts of Information and Data Governance were reviewed, published on the council's training system and are now incorporated into the Personal Development Programme.

Some of our compliancy requirements require us to demonstrate 95% of staff are trained and following a council wide campaign by the end of December 2022 we achieved a 98% completion of mandatory training.

Liaising with our peers, this identified that no one else has achieved this and we are now advising others on how to do it.

To maintain this the Information and Data Governance team monitors the compliance and users that do not complete the training have access to the network removed until it is done.

How we achieved it:

- Regular All Enfield communications sent directly and via Staff Matters
- We ran weekly reports to monitor compliance
- Reminders were sent to users who were non-compliant on a weekly basis.
- A separate list was sent to managers HOS Directors and Ex Directors on a weekly basis.
- Learning and Development team enabled new starters to complete training within 5 days of joining the council.

Also, any new starters joining Enfield in 2023 will be required to complete the mandated training before they are allowed full systems access.

Since the end of December, we have worked hard with staff so that the remaining 2% have now completed the training.

Cyber Training

Annual Training	
Total Staff	3301
Total Completed	3255
Total Not complete/expired	46
% Complete	98%
% Not Complete/Expired	2%

Data Protection Training

Annual Training	
Total Staff	3301
Total Completed	3252
Total Not complete/expired	49
% Complete	98%
% Not Complete/Expired	2%

8. Data Retention

The council must maintain a record of all of it electronic and paper data, what it is used for and for how long it can be retained. This information is published on the council website and staff intranet and refreshed annually.

Over the past 24 months, the schedule has been reviewed and rebuilt entirely to meet Information Governance standards. At the start of the review, there were less than 200 sets of data and less than 50% had identified a named service owner who was responsible for making sure that data was only retained for as long as allowed.

By the end of 2022/23 the schedule will contain 466 different sets of data, of which 98% will have a named service owner. This significantly reduces the risk that information and data entrusted to us is used incorrectly.

A further benefit, is that changes to system or data use are measured against the impact within the Data Retention Schedule including any contract awards that affect data use, ensuring that our suppliers are also compliant when holding or using our data.

9. Information and Data Governance Policies

There are now 21 policies in the Council that support Information and Data Governance. These were all reviewed by the end of April 2022.
These are reviewed annually or when a change or new need arises and there is one new policy added for Email retention.

Policy Name	Responsible Service
Acceptable Use Policy	Information and Data Governance
Access Control Policy	Security
Bring Your Own Device Policy	Information and Data Governance
Clear Desk and Clear Screen Policy	Information and Data Governance
Cyber Security Policy	Security
Data Protection Policy	DPO
Email Retention Policy	Information and Data Governance
Freedom of Information Policy	Complaints Team
Information Classification and Handling Policy	Information and Data Governance
Information Management Strategy	Information and Data Governance
IT Operations and Network Policy	Information and Data Governance
Members Information Security Policy Agreement	Information and Data Governance /Corporate and Cyber security
PCI DSS Policy	Information and Data

	Governance
Physical and Environmental Security Policy	Security
Record Retention Schedule	Information and Data Governance
Records Management Policy	Records Management
Software Acceptable Usage Policy	Security
Software Asset Management Policy	Security
Subject Access Policy and Procedure	Complaints Team
Third Party Access and Management Policy	Information and Data Governance
Use of Cloud Security Policy	Security
Data Quality Policy	Information and Data Governance

10. Reporting of Information and Data Governance Incidents

Incidents are reported through the council's Digital Services Portal and relate to both use of digital and paper data. These incidents are reported as either Information Governance or Cyber Security.

During 2022/23 to 20th February, there have been 271 incidents reported through this route. Not all of these related to Information and Data Governance, but of those that have been identified none have been high risk, and the incidents have been resolved.

11. Information and Data Governance Team

Data Governance is now part of the Information Governance team, which means that there is now one place that has oversight on data and information whether it is held digitally or paper. A dedicated Data Governance Officer is being recruited at the time of this report.

This builds on many previous improvements addressed over the past 18 months.

- Dedicated Intranet space for Information and Data Governance including access to all Information and Data Governance policy
- Information and Data Governance Policies and information publicly accessible through council's web page
- Annual reviews of Information and Data Retention to ensure compliance including reporting
- Reviews of privacy statements
- Risk process updated to ensure information and data governance risks are captured specifically and are supported by risk assessment process, examples have included Working from Abroad, data shared on social media and video conferencing tools
- Monthly reporting on Information and Data Governance
- A compliancy calendar to ensure standards and statutory compliance is reviewed and maintained

- Data Sharing Agreements now completed and reviewed following a single process which keeps council compliant and aware the data and information it can share and use

12. There is a Digital Implications process in place for any technology change, which includes consideration of impact on Information and Data Governance, including any new contracts to be awarded. Recent cyber incidents have indicated we may want to take a broader approach in other wider Council changes and new contracts. We will be reviewing options for this in the next period.

13. Working with Peer Organisations

    During 2022 the council was approached by and started working closely with the Local Government Association and London Council's following its innovative work around Information and Data Governance, Cyber Security and Digital Inclusion.

    The council continues to be a key member of Information and Governance (IGFL) for London, London Office of Technology and Innovation (LOTI), Information Security for London (ISFL) and works closely with National Cyber Security Centre.

    We now undertake collaborative working them including testing of simulation of Cyber-attack and preparation of over 25 pan-London Data Sharing Agreements.

14. Cyber Security

    Since the implementation of the Security Assurance Board in 2021, there have been many iterative improvements in how this is managed, including to the creation of a standalone Digital Security Service to increase focus and resources to treat these risks. The council also have a Security team in place across the Corporate and Cyber functions and the new Head of Corporate and Cyber Security started in January 2023.

    We also introduced the role of a Chief Information Security Officer (CISO) as part of the duties of the Director of Digital, Data and Technology advising on best practice. A separate report goes to Assurance Board and GPC to update on the security posture for the council.

15. Data Protection Officer

    The Data Protection role remains as an independent and advisory role reporting to Head of Audit and Risk to follow independent best practice. This is now embedded, and the Data Protection Officer and team are a key part of the Information and Data Governance Board.

Preferred Option and Reasons for Preferred Option

16. Building on the past year's progress, Information and Data Governance has continued to improve the monitoring, dashboard reporting, reviewing and improvement of policies and education and awareness.

    With the introduction of the Covid Public Inquiry and there is a need to ensure that the retention of and treatment of that information answers any

requests made. As the terms of the inquiry become wider, it is becoming clear that some of our existing policies and rules around retention of information may need to change. For example, we may be asked to retain information until the Inquiry finishes and that may be different than our policies currently say. By monitoring and agreeing any changes via the board, this will provide assurance that these are applied correctly and consistently.

We will continue to maintain the progress made and address the following:

Information and Data Governance Board will review the Terms of Reference, so it incorporates Data Governance and Quality and for as long as required, it will include the Covid Inquiry as a dedicated item and set of standards and continue to:

- Review and Sign Off Compliance
- Review threats and the Information and Data Governance items on the risk register
- Review performance against each of the reporting areas
- Review Audit Observations
- Review best practice and policy
- Ensure raised awareness, communication, development and training are in place
- Corporate Dashboard of Information and Data Governance Information
- Raise awareness to Assurance Board

A new annual plan will be agreed by the Information and Data Governance Board in April 2023 and published shortly after to reflect this, including a dashboard of information to held centrally and a campaign undertaken to reinforce and continue to raise awareness of Information and Data Governance covering the following.

- Statutory Compliance
- Standards
- Data Retention and removal
- Ownership of data
- Data Quality
- Paper records
- Assurance
- Best practice and policies
- Testing of compliance
- Identifying standards to benchmark against

Working with the new Head of Corporate and Cyber Security we will review our policies and reporting specifically for paper and office based information. Following the successful approach around education and awareness regarding mandatory training, there will be specific campaign aimed at raising awareness around this information.

This will enable the board to monitor and ensure delivery of the following:

- The continuing impact of changes on the information and data that council collects, processes and retains and the need to amend and adapt at speed while maintaining policies and compliance that still fit the model.
- The increased requirement for education, awareness and mandatory training to ensure the council maintains compliance with statutory and best practice standards
- The alignment of Information and Data Governance within the Digital Services Strategy and the need to identify benchmarking standards during which we then look to implement in 2023/24.
- To maintain and improve its standards, the council will need to continue to invest in its' training, awareness and applications to being able keep pace with changes in Information and Data Governance to remain compliant.
- Failure to evolve the scrutiny, measure compliance and the tools used to ensure that the council looks after its' residents and customers' information will place the organisation and its officers at risk of non-compliance and national scrutiny including both financial and reputational risk.

17. Risks that may arise if the proposed decision and related work is not taken

- Non-compliance with Information and Data Governance policies and standards puts the council at risk of financial penalties and reputational damage.
- Significant Financial Impact for the whole council if we do not comply with policies and are fined.
- Staff and organisational awareness of Information and Data Governance risks and compliance will not be embedded
- The organisation will not have the processes or scrutiny to deal with a changing way of delivering services
- The impact of increasing cyber security threats will not be embedded in the risk process for Information and Data Governance
- Staff cultural awareness of cyber security risks will not be embedded in the organisation.
- Suppliers may not deal with us if they see we are not compliant or have a poor reputation, impacting on service delivery and cost.

18. Risks that may arise if the proposed decision is taken and actions that will be taken to manage these risks

    - Information and Data Governance and Data Protection compliance will remain a risk. Driven by factors ranging from cyber security attacks to human error in disclosure. The proposed scrutiny and reporting to the Information and Data Governance Board will assist in identifying risk and how to mitigate these risks, along with the ongoing review of processes.

19. To conclude, the council has committed to the delivery of a Cyber Security Remediation Programme and implemented a supporting structure to mitigate risks, maintain compliance and keep ahead of emerging threats. We have also introduced a more robust review of Data Policies, Governance and checking of compliance by engaging with the business on retention periods, which is endorsed by the significant number of audit or compliance actions raised in the past 12 months, any breaches of policy are now investigated quickly and actioned in a pragmatic and responsive, educating way. We are making good to excellent progress with no red or critical issues and a handful of amber.

    By delivering that programme, it will provide a basis to raise standards to enable the organisation to attempt to achieve ISO accreditation in the future. It requires the entire organisation to understand it's responsibility to comply with, support and raise awareness and to help Digital Services in keeping the organisation compliant, secure and safe.

Relevance to Council Plans and Strategies

20. Managing Information and Data Governance and ensures the council fulfils its' statutory requirements and contributes to the Council's ability to address the values set out within the Council's plan

Financial Implications

21. The financial implications of the Information and Data Governance are funded through the existing Digital Services budgets. As new software and requirements emerge this will be addressed via the medium-term financial plan and capital programme; Please note that the financial implications of non-compliance can result in a fine of up to a maximum of £17.5m or 4% of turnover.

Other Implications

22. IT/Technical/Digital Services Implications are covered within the report and within the risks.

Report Author: **Martin Sanders**
Head of Service Management and Governance
[**martin.sanders@enfield.gov.uk**]
[**02081320061**

Appendices
NONE

Background Papers
INFORMATION GOVERNANCE BOARD MINUTES 2022-23

#Departmental reference number, if relevant: N/A