London Borough of Enfield

General Purposes Committee

4 March 2021

Subject: **Information Governance & GDPR Implementation**
Cabinet Member:
Executive Director: Fay Hammond, Executive Director Resources

Key Decision: **Councillor Mary Maguire**

Purpose of Report

This report provides the sets the annual summary of the Information Governance Board and the compliance with GDPR for organisation.

Proposal(s)

1. To recognise and accept the findings in this report.
2. To recognise and accept the progress of and plans of the Information Governance Board.
3. To agree the closure of GDPR Implementation and move into standard delivery and scrutiny

Reason for Proposal(s)

4. This report provides assurance of Information Governance.
5. This report provides the existing assurance levels including local reporting.
6. Increased Remote Working requires additional scrutiny on dealing with Information
7. To explain the approach for data and paper information and monitoring compliance with retention policy
8. To maintain statutory compliance the council needs to ensure its monitoring processes, tools and data is adhered to by all those that handle it.
9. The whole council needs be aware of the handling information, the policies and risks of non-compliance. An awareness programme and training to be implemented.

Relevance to the Council Plan

10. Managing Information Governance and compliance with GDPR Regulations 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

Background

11. Information Governance Board

The Information 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 Legal Services, Information Governance, Security, Knowledge and Insights, Complaints and Data Protection.

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

12. GDPR Compliance

The GDPR (General Data Protection Regulations) framework started on 25th May 2018, replacing the previous 1995 Data Protection directive.

In 2017 the council commenced implementation of the new framework in readiness for 25th May 2018 and since then has established processes, monitoring and set up a service to oversee Data Protection.

Reporting and compliance is included in the Assurance Board reporting and reported monthly to the Information Governance Board.

13. Impact of pandemic on Information Governance and GDPR

As referenced in the Cyber Security reports brought to the General Purposes Committee in July 2020 and November 2020, the significant increase in remote working (up by nearly 500%) in the organisation has provided some challenges and opportunities in how we deal with and report on Information Governance and GDPR.

Our Cyber Security Remediation Programme is dealing with these challenges in a holistic way, ensuring that technology, security, compliance, information and data is looked at together so any improvements and changes can be made as one. That plan is on track for delivery by the end of Q1 2021/22.

There are specific challenges that the pandemic has created:

- Increased homeworking and protecting data and information at home
- Changes in where staff are located, particularly when dealing with front line services and collecting or sharing data
- Lack of onsite staff, and ensuring that data remains secure
- The accelerated move from paper to electronic data
- The increased use of video conferencing, including introducing new tools such as Zoom or holding public meetings on line
- The speed of change in delivery or guidance and the impact on assessing risk and providing solutions at speed
- Incidents that have affected peer organisations such as the Hackney Ransomware attack, that has caused organisations to assess its readiness to deal with such an incident

14. Improvements and Changes within the organisation

Creation of Information Governance Team

In January 2020, Digital Services (formerly ICT) created a dedicated team recruiting an experienced Information Governance Manager, reporting into Head of Service Management and Governance. This teams purpose is to set standards, monitor compliance, raise awareness within the organisation and assess and introduce improvements and changes.

Working with Peer Organisations and benchmarking

In addition to the National Cyber Security Centre Standards being implemented from June 2020, the Information Governance Standards of the organisation are being developed with peer groups. To do this, Enfield is a key member of Information Governance for London (IGFL) which meets weekly to improve awareness across peer groups, develop best practice and shares ideas and support.

Digital Services Reorganisation and Strategy

The reorganisation and strategy were signed off and commenced implementation in November 2020.

As a result, the Head of Service Management and Governance, is now responsible for overseeing Information Governance aligning this with Cyber Security ensuring a joined-up approach to standards, delivery and monitoring.

The reorganisation and the Digital Services strategy will enable the organisation to look to achieve ISO Standards in the year 2022/23.

In addition, the Knowledge and Insights Service was also moved into Digital Services ensuring that Data Quality reports to the same Director.

Review of the Data Protection Officer role

To ensure the Data Protection role remains as an independent and advisory role, the DPO role is being moved from reporting to Head of

Service Management and Governance to Head of Audit and Risk to avoid any conflicts of interest and following independent best practice.

In addition, the council has recruited and offered the DPO post to a permanent officer, who is expected to start in March. The current DPO role is covered by a contract with Ex Cathedra Solutions and this ends at the end of April and there will be a full handover to the permanent officer.

15. Information Governance Board – last 12 months

Highlights

Amended Terms of Reference to incorporate new standards and policies for Data Quality and retention of data to include paper

Information Governance Policies reviewed by April 2020

Social Media and Video Conferencing Information Governance introduced

Handover of Chair and Running of Board from Head of Legal Services to Head of Service Management and Governance

Learning and Development engagement to develop a set of on line tools to ensure development, training and awareness is improved

Incorporation of Information Governance improvements that complement Cyber Security into Cyber Security Remediation Programme to be delivered by end of Q1 2021/22

Paper retention and disposal audit commenced in December 2020 report to IGB by April 2021.

Data retention schedule and policies updated for best practice and compliance review commenced in February 2021. Non-compliance to be reviewed and overseen by IGB, April 2021 and reported to Assurance Board.

Standard IGB reporting on DPO, Complaints, MEQ and FOI

Third Party Data Sharing review added into annual schedule of reviews, particularly considering the impact on both Cyber Security but existing contracted terms of suppliers to comply with our Security and Information Governance Standards

Next Steps

Over the past 12 months the scale of Information Governance and best practice across the organisation has been highlighted. The introduction of dedicated staff to work in this area, the impact of increased remote working and accompanying changes to service delivery, a new Digital Services structure and strategy and by bringing together Information Governance and Cyber Security has provided challenges and opportunities that IGB can address.

- A clear annual plan to review compliance against key information governance risks
  - Statutory Compliance
  - Standards
  - Data Retention and removal
  - Ownership of data
  - Paper records
  - Assurance
  - Best practice and policies

- The role of IGB to focus on
  - Review and Sign Off Compliance
  - Review threats and the Information Governance and GDPR items on the risk register
  - Review Audit Observations
  - Review best practice and policy
  - Ensure raised awareness, communication, development and training are in place
  - Corporate Dashboard of Information Governance Information

- To raise standards and aim to achieve accreditation for Information Governance processes and standards
  - In line with the Digital Services Strategy to baseline by the end of 21/22 so that the organisation can plan and prepare for achieving ISO standards within 22/23 and to have achieved the standard by 23/24

16. GDPR Implementation

Enfield Council successfully implemented changes so it was compliant with GDPR regulations by 25th May 2018. Since then it has implemented processes, structure and training to ensure it remains compliant and undertakes the relevant reporting of any breaches or issues.

The Data Protection Officer reports performance and risk monthly to the Information Governance Board and in addition provides reports to the council’s assurance board.

Incidents Summary

There were 3 incidents reported to the Information Commissioners Office in the past 12 months. All were closed with no further action taken.

Email errors continue to be the dominant problems accounting for 83% incidents in Feb 2020-Jan 2021. These include:

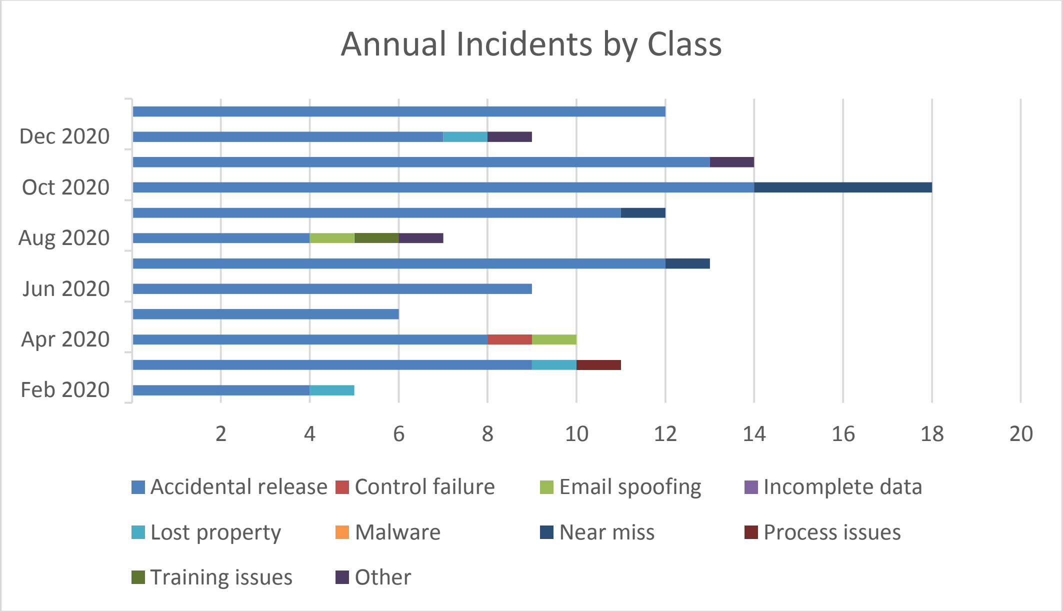
- Sending to wrong person(s) via autocomplete
- Sending to inappropriate persons via incorrect selection of mailing list
- Not using BCC and allowing email addresses to be leaked
- Including information not intended for all recipients

Since the pandemic and increased remote working there has been a surge in phishing emails received by the council in line with other peer organisations. These are attempts to obtain details via diverting users to fake sites asking for personal information such as bank details or asking users to install fake applications.

In addition to software and tools in place to spot and prevent such attempts, this has also been complemented by a continuous Cyber and Information Governance awareness programme across the organisation, undertaking simulated test attacks to check that our processes work, using internal corporate communications, the deployment of screen savers and tips of the day and a single go to place for information on the council's intranet.

The on-going raising of awareness has been complemented by new learning and development tools and training, alongside the Information Governance Manager leading on setting up working groups and networks to review outcomes should enforce the importance of compliance with GDPR and Information Governance standards.

Data Protection Incidents February 2020 to January 2021



Cause	Feb 2020	Mar 2020	Apr 2020	May 2020	Jun 2020	Jul 2020	Aug 2020	Sept 2020	Oct 2020	Nov 2020	Dec 2020	Jan 2021	Total	% of total
Accidental release	3	6	6	3	4	4	4	8	13	11	6	7	**75**	**83%**
Control failure			1										**1**	**1%**
Email spoofing			1				1						**2**	**2%**
Incomplete data														
Lost property	1	1											**2**	**2%**
Malware														
Near miss						1		1	4				**6**	**7%**
Process issues		1											**1**	**1%**
Resource issues														
Training issues							1						**1**	**1%**
Other							1			1			**2**	**2%**
Total	**4**	**8**	**8**	**3**	**4**	**5**	**7**	**9**	**17**	**12**	**6**	**7**	**90**	**100%**

Main Considerations for the Council

17. The impact of the pandemic on how the council processes and retains information and the need to amend and adapt at speed while maintaining policies and compliance that still fit the model.

18. The proposed changes to the role of the Information Governance Board and it’s expanded scrutiny to incorporate Data Quality and Paper Retention and Disposal

19. The alignment with and complementary role to Cyber Security Remediation and Assurance

20. The alignment of Information Governance within the Digital Services Strategy and particularly the aspiration to prepare for accreditation in 2022/23 and achieve by 2023/24.

21. To acknowledge that GDPR Implementation is complete and that we move into using the Information Governance Board to monitor and provide assurance on Data Protection Officer.

22. 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 Governance and GDPR to remain compliant.

23. 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.

Safeguarding Implications

24. Maintaining compliant Information Governance is essential to all services we support and in particular services for children, young people and vulnerable adults. This report seeks to demonstrate the existing position

for the organisation and its' proposed way forward to maintain compliance and reduce risks.

Public Health Implications

25. Service delivery requires compliant and secure Information Governance, this includes any services delivering public health. This report seeks to demonstrate the existing position for the organisation and its' proposed way forward to maintain compliance and reduce risks.

Equalities Impact of the Proposal

26. There are no impacts from this report

Environmental and Climate Change Considerations

27. This report covers work carried out within the existing service areas and staff without any change on property use or energy consumption or carbon emissions or impact on environmental management.

28. This report does not require or request any funding or approval of contracts.

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

29. Non-compliance with Information Governance and GDPR puts the council at risk of financial penalties and reputational damage.

30. Significant Financial Impact for the whole council if we do not comply with policy and are fined.

31. Staff and organisational awareness of Information Governance risks and compliance will not be embedded

32. The organisation will not have the processes or scrutiny to deal with a changing way of delivering services

33. The impact of increasing cyber security threats will not be embedded in the risk process for Information Governance

34. Staff cultural awareness of cyber security risks will not be embedded in the organisation.

35. Suppliers may not deal with us if they see we are not compliant or have a poor reputation, impacting on service delivery and cost.

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

36. Information 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 Governance Board will assist in identifying risk and how to mitigate these risks, along with the ongoing review of processes.

Financial Implications

37. The financial implications of the Information 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.

Legal Implications

38. None

Workforce Implications

39. None

Property Implications

40. None

Other Implications

41. ICT Implications are covered within the report and within the risks.

Options Considered

42. Do Nothing was not considered as Enfield would lose its' statutory compliance certifications and put its' entire network and services at risk

Conclusions

The council has committed to delivery of a Cyber Security Remediation Programme and implemented a supporting structure to mitigate risks, maintain compliance and keep ahead of emerging threats.

By delivering that programme, it will provide a basis to raise standards to be ready to achieve ISO accreditation on 2022/23 onwards. 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.

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

Date of report: 04 March 2021

Background Papers

The following documents have been relied on in the preparation of this report:

General Purposes Committee meeting, 23 July 2020 (Cyber & Technology Security, agenda item 7)

General Purposes Committee Meeting, 26 November202023 July 2020 (Cyber & Technology Security update, agenda item 7)