Report to the Audit Committee

28 September 2020

Wards: All

Annual Information Governance Report

Report of the: Information and Data Protection Manager & Head of ICT Operations and Support

This item is not exempt
Therefore exempt reasons are not applicable

This is a Non-Key Decision

1. Purpose of the Report and Summary

1.1 The Audit Committee holds the key roles of overseeing the Council's arrangements for corporate governance and agreeing necessary actions to ensure compliance with best practice and providing its endorsement of the Annual Governance Statement prior to signing. To inform that role it is appropriate that the Committee receives reports upon the Council's Information Governance activity.

1.2 The Council's Information Governance Group (IGG) provides officer oversight and direction on information management matters to provide assurance in the areas of information governance, information security and information rights. This report details the work of the Information Governance Group (IGG) for January 2019 – December 2019.

2. Recommendations

2.1 The Audit Committee is asked to note the measures taken to ensure effective Information Governance in relation to Information and Data Management within the Council as set out within the report

2.2 That the Audit Committee continues to receive an annual report to inform its role in endorsing the Annual Governance

Statement.

3. Reasons for Recommendations

3.1 The proposals within the report provide assurance upon the arrangements established for the management of information and data within the Council.

4. Impact on other Executive Committees (including Area Committees)

4.1 None

5. Background

5.1 The Council has established an officer Information Governance Group to manage Information Governance compliance and risk management within the Council.

5.2 Information Governance Group
The IGG meets monthly to co-ordinate information governance activity to ensure the council meets its obligations to keep information safe, accurate and accessible. The Group is chaired by the Director of Legal Services and Partnerships, who is also the Council's Senior Information Risk Owner, and the Secretary to the Group is the Information and Data Protection Officer.

5.3 Areas of activity have included the following:

5.4 NHS Data Security Protection Toolkit (DSPT)

The NHS DSPT is a national standard defining requirements and rules for the creation and transport of electronic information within a set of common specifications, frameworks and implementation guides that support interoperability. Interoperability is the enabling of computers to talk to one another.

In some areas there is a good level of similarity in business process, data requirements and technical alignment. In some areas solutions compete or incompatible. The DSPT seeks to solve these problems by providing a number of specifications and technologies which are consistent and applicable across a wide range of domains and localities to reduce expenditure in integration, reduce delivery times for implementation and allow the benefits of interoperability to be scaled.

5.5 The Council has an established framework for the management of information with Health bodies to ensure the protection of the welfare of clients and the development of effective measures to s services needs to be able to share data

5.6 This area of activity is of increasing importance as the Council develops systems for Health and Social Care Integration in accordance with the principles of the Health and Social Care Act 2012.

5.7 To demonstrate compliance the Council is normally required to provide an annual submission at the end of March each year, however, due to the Covid-19 crisis the deadline for the 20/21 DSPT has been pushed back to September. As a social care provider the Council is required to complete the Local Authority version of the toolkit to cover its Adult Social Care and Public Health Services.

5.8 Integration of Health and Social Care

The Council's Data Protection Officer has been appointed by the NHS Hull Clinical Commissioning Group to also fulfil the role of Data Protection Officer for the Clinical Commissioning Group. This has supported joined up service delivery enabling a consistent approach across the Health and Social Care System, particularly where the Council and the CCG are both supporting a client (e.g. Continuing Health Care). In this role the Council's Data Protection Officer works closely with the CCG's Information Governance lead and attends their Information Governance Steering Group meetings.

5.9 Cabinet Office requirements for wider Government Information Sharing - Public Services Network (PSN) accreditation

To enable the Council to retain access to services on the Government Services Intranet including secure Gov. and the DWP Customer Information System the Council must have in place Public Services Network (PSN) accreditation. The Council is required to provide an annual submission to the Cabinet Office to meet standards which increase each year. The annual PSN accreditation application is prepared for submission through the Council's ICT & Digital Service with oversight from the Director of Legal Services and Partnerships, IGG, SIRO and the Chief Executive. External auditing is undertaken through the Cabinet Office as part of the PSN re-accreditation process. The requirements are updated each year reflecting changes in software licensing and security standards.

5.10 Future Networks for Government

The Cabinet Office continues to plan for when Government services are accessed and data is shared securely via the Internet, and when the PSN network is no longer needed. A draft timeline for PSN closedown recently published suggests this may take place as early as 2023.

This has implications for information sharing and access to systems, and for ongoing assurance that the Council is maintaining effective cybersecurity, as the yearly technical audit performed by external specialist – the IT Health Check – will no longer be required as part of the PSN accreditation process, however HCC will continue to have yearly accredited IT Heath Checks.

ICT & Digital has implemented a dedicated Cybersecurity Team and is currently designing policies and processes to ensure future decommissioning takes place effectively, that a sufficient level of security is maintained beyond PSN termination, and that responsibilities to partner organisations and secure information sharing are maintained.

5.11 Monitoring of Information Security Incidents

IGG reviews actual or suspected information security breaches and 'near-misses' each month. This provides assurance that the Information Governance Team is properly investigating and resolving incidents and allows 'lessons learned' to be applied to the wider organisation.

191 incidents (confirmed or suspected breaches, near-misses and concerns) were reported and investigated during the period compared to 198 for the preceding 12 months. Information security awareness work has continued throughout this period. IGG will continue to review individual incidents and wider reporting trends at its monthly meetings and is very aware of the potential problem of staff awareness and underreporting of incidents.

The ICO has not taken any action against the Council for breaches of data protection in the period.

5.12 Monitoring of ICO Information Rights Concerns

IGG monitors complaints against the Council on information rights matters, primarily Freedom of Information and Data Protection Act Subject Access Requests. There was 1 ICO decision notices in

respect of the Council in 2019 (1 in 2018).

In this case the applicant had requested details of all properties which provide supported accommodation on 11 streets in the city. The list was provided but the applicant complained that they had done their own research with landlords in the area and their figures were different.

The decision was reviewed by the Council who explained that the figures that had been provided were an accurate reflection of the data held by the Council at the time the request was submitted but the only place this data is held is the Housing Benefit system. It was explained that where supported accommodation is being let to tenants who are not claiming Housing Benefit the Council would have no record of the properties being used for this purpose.

The applicant made a subsequent complaint to the Information Commissioner's Office. The ICO did not uphold the complaint against the Council and concluded that –

"*On the explanations provided by the council, the Commissioner is satisfied that on the balance of probabilities, the council has provided the complainant with the information it held, at the time, relevant to the scope of the request."*

5.13 Cybersecurity Incidents

IGG reviews significant Cybersecurity Incidents which affect Council systems and services as notified by ICT & Digital's Cybersecurity Team, who oversee incident management processes to ensure response and recovery measures are effective, and that relevant internal and external stakeholders, including Law Enforcement, are notified.

5.14 Data Protection Policy Update, Training and Awareness Work

The Data Protection Policy was agreed with IGG, CST, Portfolio Holder and union representatives to ensure stakeholders were able to comment on proposed changes. The latest version of the Policy was introduced in October 2018 to include updated guidance from the ICO in view of GDPR changes. The e-learning quiz which tests knowledge of the Data Protection Policy has also been implemented and this ensures the Council can evidence its staff have read and understood the policy. Staff are automatically enrolled on the Oracle Learning Management system and are required to complete the training every 12 months. An update to the policy is anticipated in the first half of 2021 once EU exit arrangements have been finalised and any resulting changes to UK data protection rules have been

made.

Additionally, the Local Government Association has funded cybersecurity awareness support and an email 'phishing' simulation service, which will help support and educate all staff to cybersecurity threats, and particularly email scams, over the coming 12 months.

5.15 Data Protection and Information Security for Elected Members

The Information and Data Protection Manager last provided training to elected members during May 2019. Attendees included new members and any established members who felt they needed a refresher. The sessions included advice on information security and data protection risks along with an explanation of their responsibilities for information on constituency matters. The offer of training on data protection and/or information security remains open to all elected members. The Member Development & Support Team Leader is able to request and arrange training upon request.

All new members are required to attend the data protection/information security briefing at the point they are issued with their ICT equipment as a requirement of our network security accreditation.

5.16 Research Governance Process

IGG oversees the Council's Research Governance process which sets standards for research, ensures compliance with the Council's data protection and information security policies and ensures safeguarding implications of research proposals are properly considered. Some applications are relatively simple and are dealt within the relevant Directorate with more complex applications escalated to the Corporate Review Panel, a sub-committee of IGG chaired by SIRO. Most applications relate to work in CYPFS and only small numbers are received each year.

5.17 The GDPR (EU General Data Protection Regulation)

IGG's oversees the Council's compliance with the EU GDPR which took effect from 25th May 2018, along with the UK Data Protection Act 2018 which includes some additional requirements and provides some exemptions from the GDPR. Significant areas of work in 2019 included –

5.18 Data Protection Impact Assessments (DPIA's)
The IGG provides review and oversight of the Council's DPIA's. These assessments are undertaken prior to any new projects or initiatives which may pose a high risk to personal data held by the

Council. The requirement is for Privacy by Design and Default, to be managed through Data Protection Impact Assessments undertaken in advance of processing of data. The Council was already undertaking PIA's ('Privacy Impact Assessments') prior to GDPR but this process is now known as DPIA's (Data Protection Impact Assessments) to align with GDPR terminology.
A summary of the DPIA's approved during 2019 are included at Appendix A.

5.19 Supply Chain Risk Management

IGG has appraised a Supply Chain Risk Management process implemented by ICT & Digital, in collaboration with Legal and Procurement, which complements the DPIA process and aims to ensure suppliers, and systems procured, meet GDPR and cybersecurity requirements, and that risks to Information and related assets are understood and managed.

6. Risk Assessment

6.1 The Team received 1454 FOI & EIR requests in the calendar year 2019 and 80.39% were answered within the 20-day time limit. This was a 3.6% decrease on the 1509 FOI requests received in 2018 (84.74% answered within 20 days).

The ICO has indicated that it expects a minimum of 85% of requests to be completed within the 20-day deadline and IGG was briefed on the pressures on the IG Team through its monthly meetings. Increased workload supporting the Legal Service with Public Interest Immunity disclosures to the Police was the principal cause of the stress upon the Team. This was addressed through the appointment of a Grade 3 to the team to assist in the time consuming clerical work.

6.2 The Information Governance Team dealt with 2619 total work items in 2019 an increase of 7.8% on the 2429 in 2018. The main areas of work in 2018 were:

- FOI & EIR – 1454
- DPA (Other)NHS 'lost contact' children/Police) – 276
- DPA Advice – 137
- DPA Subject Access – 250
- Data Sharing – 17
- Info Security Advice/Investigations – 355
- Internal Review/Appeal – 16
- Public Interest Immunity (child care prosecutions) – 155

The remainder were logged as 'Admin & Support', 'Business As Usual' or 'Policy & Training'.

7. Information Risks/Threats/Issues in 2020/21

It is the opinion of the Information Governance Manager & Member Information Manager that the following represent information governance risks/challenges for the next 6-12 months:

7.1 **Increasing workloads in the Information Governance Team leading to reduced performance against statutory performance targets**

Mitigation: The Public Interest Immunity (PII) disclosure cases inherited from children's social care are significant area of additional work for the team. An Information Governance apprentice was employed during August 2017 to relieve the Information Governance Officer's from much of the administrative work around the PII cases. Funds were secured to recruit a permanent Information Governance Assistant who was appointed during Q3 2018/19.

7.2 **Transfer of child social care subject access requests**

Mitigation: The Information Governance Team has taken over the child social care subject access requests from June 2020. These were previously handled within CYPFS but service reorganisation led to a decision to move the function to the central IG Team. The team does not have significant social care experience to aid decisions on disclosure but staff have been provided with access to the social care system and are able to access support through social workers and the Caldicott Guardian on complex disclosure decisions.

7.3 **Impact of budget savings on ability to deliver Information Governance activity.**

Mitigation: The Information Governance Manager secured £37,000 of income from external training and assurance services in 2019. It is hoped that this business can be maintained though a large number of schools and academies joined the service to prepare for GDPR and some may not wish to retain the service in the longer term. This income generating activity does further impact performance against statutory FOI/DPA targets as well the time spent on strategic information risk management.

7.4 **Organisational changes result in the Information Governance Team's service area representatives leaving and/or changes to service structures make it more difficult to respond to statutory deadlines on information requests**

Mitigation: Assistant Directors continue to provide support by nominating capable service area representatives to liaise with the IG Team. Change management processes are in place to minimise risks around building moves and personnel exiting the organisation and transformation processes include

Information Governance as an area for consideration.

7.5 **Digital innovation and increased partnership working**

Mitigation: The Data Protection Impact Assessment process is embedded in the organisation and is included in the Data Protection & Confidentiality Policy and the annual staff training. Where personal information will be used for new initiatives or in new ways or on new systems, the DPIA process ensures that appropriate privacy and security processes are identified before processing of personal information begins.

7.6 **Impact of Covid-19 upon services**

Mitigation: Significant stress was placed upon frontline services as the Council needed to respond to the crisis and keep residents safe and secure. Given the need to act quickly to address the needs of shielding residents it was not possible to ensure the normal level of oversight on the changes to how we processed personal data. Some measures, such as the implementation of the portal for residents to request assistance and the support packages had to be implemented without a data protection impact assessment being completed in advance. The Information and Data Protection Manager worked closely with Customer Services and Housing colleagues to get systems in place quickly while ensuring that processing remained safe, fair and lawful. However, it was only 2 months later when the data protection impact assessment was presented to IGG for consideration – normally IGG would see a proposal and be able to provide comments and feedback before it goes live. The Information Commissioner's Office published statements at the time which made clear that it accepted that where measures needed to be implemented quickly the normal levels of oversight may have to be relaxed until immediate pressures eased and it was possible to review the activity in more detail. The Council was forced to take this approach but no security breaches are known to have resulted from the changes implemented to support residents during the crisis and data protection impact assessments were completed as soon as reasonably possible afterwards.

7.7 **Automated decision-making using personal data**

Automated processing is increasingly used in business, including within public sector organisations. The profile of automated decision-making is increasing and it is important that where the Council chooses to implement any such processing that it does so in a lawful and transparent manner. The use of automated decision-making has come into sharp focus after an

algorithm used by the exam regulator Ofqual downgraded almost 40% of the A-level grades assessed by teachers.

The Council currently has limited automated decision-making in use as part of the risk based verification process for Housing Benefit claims. Cases are selected for additional human scrutiny based upon a computer algorithm. Although no final decisions on entitlement are made by purely automated means the decision to subject claims to additional scrutiny is entirely automated. It is recommended that the Civica, who operate the system on behalf of the Council be asked to review the arrangements and justify the continued use of this automated process. It should be noted that the system is relatively widely used by local authorities and the Housing Benefit privacy notice is published online and includes details of this process.

Housing also uses some limited automated decision-making. The system predicts cases where tenants are likely to fall into arrears and they are proactively contacted with offers of support to help safeguard their tenancy. All tenants where made aware of the scheme in advance and offered the opportunity to opt-out. Each time a tenant is contacted they are reminded of how to opt-out of the service.

For many years the Audit and Fraud service manually accessed various Council systems as part of their core anti-fraud work. They now run reports using the Council's Master Data Management system to identify anomalies across various internal systems for further investigation. This is a logical refinement of the previous manual searches and data comparison work undertaken by the Audit and Fraud Service. The Council already provides such data to the Cabinet Office in regular extracts to support the work of the National Anti-Fraud Initiative in accordance with the Local Audit and Accountability Act 2014.

7.8 **Cybersecurity Incidents**

The Cybersecurity Team supported incident management for a number of events, and 4 significant incidents in the calendar year 2019 - in summary, as follows:

- A cybersecurity breach of a 3rd party procured system – with no indication of data loss/theft.

- A vulnerability with a hosted website developed by a 3rd party, as notified to us by the National Cyber Security Centre – with no indication of data loss/theft.

- A significant attack on an element of Cloud infrastructure which was possible due to mistakes made by a 3rd party service provider – with no indication of data loss / theft.

- An email 'phishing' campaign that successfully infected a number of

users with malicious software – a forensic review by external specialists established that some email related data was lost from specific users, which did include a limited amount of private data.

In each case Information Governance provided support and guidance, IGG provided oversight, the ICO were notified where necessary, the National Cyber Security Centre was consulted, and where a crime was suspected, the Police were informed.

All external suppliers were engaged and, where appropriate, consulted on their security provision and reminded of their obligations – with further assurances sought.

Equally, 'Lessons Learned' from these incidents were reviewed to inform ongoing improvements, and these processes will be further strengthened via a wider framework, as outlined elsewhere.

It's important to note that these were either significant events or breaches of security, and not just attacks. The Council is under constant cyber-attack, with, for instance, thousands of malicious emails received every week.

Whilst there have been no critical incidents experienced so far, this year has seen a greater number of cybersecurity incidents already, with 10 as of September 2020.

In any given period, the majority of attacks are not successful, yet it's widely agreed to not be possible to defend against all attacks, and so the focus is on driving down incident numbers to a minimum, and significantly reducing the impact of breaches when they do occur.

7.9 Cybersecurity Threats/Risks 2020/21

The Cybersecurity Manager foresees the following risks/challenges for the next 6-12 months:

7.9.1 Continued cybersecurity impact of COVID19

The rapid rate of response, requiring unprecedented changes to working practices and technology provision placed significant pressure on capacity, and standard risk mitigation strategies were tested, yet were maintained to protect the most sensitive assets.

For now, key risks have been identified and risk treatment strategies have been or are being implemented. This should provide some additional knowledge and capacity to meet future requirements, should a further demand increase occur.

The opportunity offered by such a crisis to cybercriminals has been exploited

widely across the public and private sectors, with a greater number of attacks having been experience locally, and by the Council.

This will very likely continue for a prolonged period, with challenges such as securing information due to home working, the use of new collaboration technologies, and Social Engineering attacks designed to deceive and defraud, remaining commonplace.

This requires all staff to remain alert – which presents its own challenges, as vigilance can wane over time. Continued awareness and communication is planned and will be maintained in an attempt to address this.

Visibility of an increase of existing and emerging cyber threats is important and will be maintained by engagement with regional partners though the Yorkshire and Humber Warning and Reporting Point (YHWARP), Central Government through the Cabinet Office, and with the National Cyber Security Centre.

Regular threat reviews and notifications will continue to be shared with relevant stakeholders, to ensure timely responses are taken whenever possible.

7.9.2 Impact of Cloud Migration Programme

The programme to migrate a majority of services and infrastructure to the Cloud has the potential to affect availability and the security of systems and data.

The inclusion of a new dedicated cybersecurity role within the Programme Team for the duration of the activity is a positive development that will complement existing resources and help ensure a clear focus on maintaining availability and security throughout the period of transition.

The existing Cybersecurity Team will work closely with the Cloud Migration Programme Team to provide support and guidance, and to ensure that relevant policies and standards reflect the changes, and the need for enhanced security as activities progress.

7.9.3 Shared Public Sector Challenges

Recent high profile events, such as the ransomware cybersecurity incident at Cleveland and Redcar Borough Council have highlighted the scale of the challenges faced by the Public Sector, and particularly Local Government, when facing the many challenges posed by Cybersecurity risks, threats and vulnerabilities.

Hull City Council is not unusual in this regard; there are commonalities across many similar organisations, with particular challenges for skills and resources, and one which the Government Digital Service (GDS) is currently

researching more thoroughly.

We have supported these wider efforts and will continue to do so, and are particularly grateful for the insights provided by a 3rd party review commissioned by the GDS of specific elements of our cybersecurity that this provided.

The Cybersecurity Team are currently reviewing and implementing a framework of activity that will address many of the challenges faced, provide a rolling plan of issue identification, and identify opportunities for continuous improvement.

In line with industry best practice this will highlight areas where further support is needed, working in collaboration with regional and national partners.

8. Comments of the Town Clerk (Monitoring Officer)

8.1 The Town Clerk has been closely involved in the development of this report and supports the recommendations.

9. Comments of the Section 151 Officer

9.1 All organisations face risks in relation to regulatory breaches in each of the areas covered by this report, as well as the potential to lose business sensitive data. Those risks carry potentially significant financial, operational and reputational consequences. The s.151 Officer therefore welcomes the mitigations and assurances that are set out in this report. [PH]

10. Comments of HR City Manager and compliance with the Equality Duty

10.1 The contents of this report are noted and will be taken into account in the development of training plans for the organisation.

11. Comments of Overview and Scrutiny

11.1 This report has not been subject to pre-decision scrutiny. (Ref. Sc5837 (FH)

Information & Data Protection Manager

Contact Officer: Jim Strangeway Telephone No.: 01482 613295

Officer Interests: None

Background Documents: -

Appendix A – Data Protection Impact Assessment Summary for June 2019 – August 2020