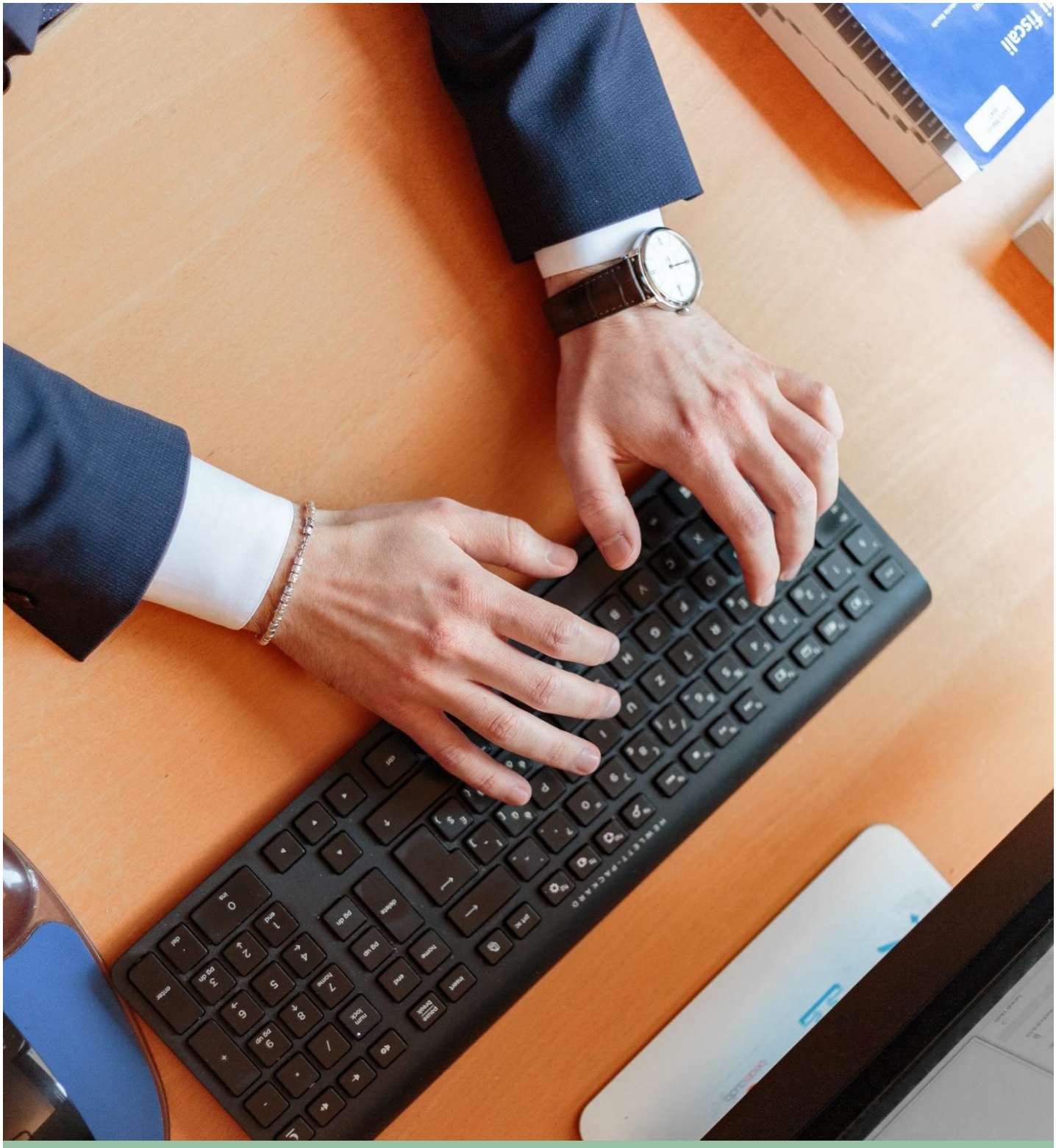
INFORMATION GOVERNANCE ANNUAL REPORT

Date: 27 July 2022

ANNEX 3



Veritau

CONTENTS

Kirsty Bewick
Assistant Director - Information Governance

Max Thomas
Head of Internal Audit

Circulation list: Members of the Audit and Governance Committee
Chief Executive
Chief Finance Officer (S151 Officer)

PURPOSE OF THE REPORT

1 To provide an update on Information Governance matters and developments in the Council's Information Governance arrangements and compliance with relevant legislation.

2 Information governance is the framework established for managing, recording, protecting, using and sharing information assets in order to support the efficient and effective delivery of services. The framework includes management structures, policies and processes, technical measures and action plans. It helps to ensure information is handled securely and correctly, and provides assurance to the public, partners and other stakeholders that the Council is complying with all statutory, regulatory and best practice requirements. Information is a key asset for the Council along with money, property and human resources, and must therefore be protected accordingly. Information governance is however the responsibility of all employees.

3 The Council must comply with relevant legislation, including:

- The Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Regulation of Investigatory Powers Act 2000

4 In March 2018, the Council appointed Veritau to be its statutory Data Protection Officer (DPO).

5 The Corporate Information Governance Group (CIGG) is responsible for overseeing information governance within the Council. The group is chaired by the Chief Finance Officer and provides overall direction and guidance on all information governance matters. CIGG also helps to support the Council's Senior Information Risk Owner (the Chief Finance Officer) to discharge their responsibilities. CIGG is currently coordinating the delivery of the UK GDPR action plan, which includes reviewing and updating the Council's information governance strategy and policy framework.

UK GDPR ACTION PLAN UPDATE

6 Progress on the 2021/22 action plan was reported to CIGG throughout the year. The action plan was updated as work was completed. Actions that were deferred from the 2020/21 action plan due to the Covid pandemic were included in the 2021/22 action plan. A new 2022/23 action plan has now been provided to the Council. This includes a detailed breakdown of actions required to achieve agreed deliverables. Due to LGR CIGG agreed that no new actions should be included in the action plan. Instead, the focus will be to address priority outstanding actions required to make the Council compliant with UK GDPR and the Data Protection Act 2018.

7 Following completion of the privacy notice review in 2020/2021, Veritau are in the process of applying relevant changes to the privacy notices via

consultation with service areas. Several privacy notices have been completed and uploaded to the Council website including Planning Policy, Complaints and Explore Heart of Yorkshire. Updates have been applied to the corporate privacy notice.

8 The following new IG policies have been completed, approved by CIGG and published onto the Council's internet.

- Information Governance and Strategy Policy – a policy to protect the Council's information, manage risk to an acceptable level and ensure data is well managed.
- Personal Privacy Policy – a policy that sets out how the Council handles the personal data of its customers, suppliers, employees, and third parties.
- Information Access and Information Rights Policy – the purpose of this policy is to ensure that the Council complies with the provisions of the Information Access rights under GDPR, the Data Protection Act 2018 and Access to Health Records Act 1990.
- Information Security Incidents Reporting Policy – a policy to ensure that the Council complies with Article 33 of the UK GDPR, and ensure all breaches of personal data are reported, investigated and, if necessary, reported to the Information Commissioner.

9 A review of the Information Asset Register (IAR) was completed on 31st March 2022, which reflects UK GDPR compliance needs and now includes columns for law enforcement processing. Apart from two service areas the register reflects all the Council's current information assets. Work is ongoing to finalise the two outstanding registers in Housing and Property Services. A further review of the IAR is planned in September in consultation with other North Yorkshire councils. This will consider alignment and consistency of information across the councils in advance of Local Government Reorganisation (LGR).

10 In 2021/22 a gap analysis of the Council's data processing contracts and information sharing agreements was completed and several areas were identified as not having sufficient information. Progress in locating and acquiring copies of documentation for review in these areas was slow. Discussions to explore the feasibility of aligning this work with the LGR workstream took place.

11 Agreement was reached to align the process to review data processing contracts with the LGR workstream for Procurement. The focus of this work is primarily on those contracts to be novated to the new organisation. This is consistent with the approach to be taken by other North Yorkshire councils.

12 A gap analysis of the Council's Information Sharing Agreements (ISAs) was completed and a number of areas of concern were identified. The areas to prioritise for immediate action have been agreed. Work is ongoing to establish what other ISAs are held. Where documentation has been received, this has been reviewed. Priority will be given to ISAs during the

autumn 2022. Actions to address gaps identified are included in the 2022/23 action plan.

TRAINING

13 Delivery of training was affected by the Covid-19 pandemic in 2020/21. It was subsequently agreed by CIGG that training sessions would recommence in 2021/22 but would be held online and in smaller groups. A training session on FOI/EIR and subject access requests was delivered for service managers in January 2022. This was followed by two online workshops about data protection impact assessments (DPIAs) in February 2022. Further bespoke training will be offered through Veritau during 2022/23 and will include new workshops on Information Incident Management, and Law Enforcement Data Processing.

14 In March 2022 CIGG agreed that the focus of internal training for 2022/23 will be to ensure all staff have completed data protection training. This includes new starters and temporary and agency staff, as part of their induction.

INFORMATION SECURITY INCIDENTS (DATA BREACHES)

15 The arrangements for rating information security incident were updated during 2021/22 following approval by CIGG. The previous RAG system was replaced by a five-level system with risks ranging from very low to very high. The rating is assigned based on a risk score assigned as part of the data breach investigation. Risks classed as high or very high are sufficiently serious to be considered for self-reporting to the Information Commissioner's Office (ICO). Some incidents are categorised as 'white'. White incidents are where there has been a failure of security safeguards, but no breach of confidentiality, integrity, or availability has actually taken place, i.e. the incident was a near miss.

16 Information Security Incidents have been reported to Veritau as required.

17 The number of Security Incidents reported to the Council and Veritau in 2020/21 are as follows:

	Very High	High	Moderate	Low	Very Low	White	Total
Q1		1		4		1	6
Q2				1	1	1	3
Q3							0
Q4				1		1	2
Total	**0**	**1**	**0**	**6**	**1**	**3**	**11**

18 There has been a reduction in the number of security incidents reported in 2021/22 from the 18 reported in 2020/21.

19 To date, Veritau have handled only one security incident in 2022/23 and this was assessed as a very low risk after investigation.

SUBJECT ACCESS REQUESTS – INTERNAL REVIEWS – FREEDOM OF INFORMATION

20 As part of a revised agreement, Veritau took over the responsibility for processing Council data protection subject access requests (DPSARs) and provision of advice on complex Freedom of Information (FOI) requests on 1st February 2022. Since February Veritau has processed eight DPSARs on behalf of the Council and provided support on six complex FOI requests.

DATA PROTECTION IMPACT ASSESSMENTS

21 Veritau supported the Council in completing several DPIAs in 2021/22 as well as providing advice on whether a DPIA was required for other projects.

22 Work is ongoing on a number of DPIAs. These include MyView, CCTV for Selby town centre, ONS data sharing, and Breathing Space (a scheme administered by Wakefield Metropolitan District Council on behalf of Selby – it offers interest free secured loans to pay for an individual's mortgage arrears and support for up to 12 months of mortgage payments).

SURVEILLANCE

23 Following extensive work undertaken in 2021/22 all actions to ensure the Council is compliant with the Surveillance Code of Practice and the Regulation of Investigatory Powers (RIPA) have been completed by Veritau. This work involved a review of current overt surveillance systems (including ensuring that all necessary DPIAs and ISAs are in place), the completion of a privacy notice for CCTV operations, a RIPA policy, and delivery of training on RIPA to Authorising Officers.

LAW ENFORCEMENT

24 An initial scoping exercise was completed to ascertain which areas of the Council might be undertaking law enforcement processing, as governed by Part 3 of the Data Protection Act 2018. Areas were mapped out as far as possible and amendments to the Information Asset Register now show areas where law enforcement processing is taking place, linking back to the relevant legislation and/or enforcement policies.

25 Documents such as the new DPIA template and guidance were also drafted to include law enforcement considerations. The review of privacy notices has taken into account changes required for law enforcement processing.

The corporate privacy notice has been updated to include information about the conditions for criminal offence data, enforcement investigations and prosecutions. The IG policy framework includes a Law Enforcement policy, and this has been published.

26 A virtual training course has also been designed on law enforcement data processing and will be offered to staff during 2022/23

TECHNOLOGY

27 Work required to ensure all IT software and hardware is compliant with UK GDPR and the Data Protection Act 2018 is progressing as part of the Council's upgrade to Office 365. Twelve business departments have transferred to O365 so far. Defined retention periods have been applied to documents as part of the change.

28 Further work to upgrade remaining departments to O365 is on hold until the merging of North Yorkshire councils Microsoft platforms through the LGR process is completed. The LGR IT and Digital Data Governance workstream is currently collating data to understand the document retention and disposal rules across all 8 Councils before creating a plan of action to implement this in a consistent way ahead of LGR next year.