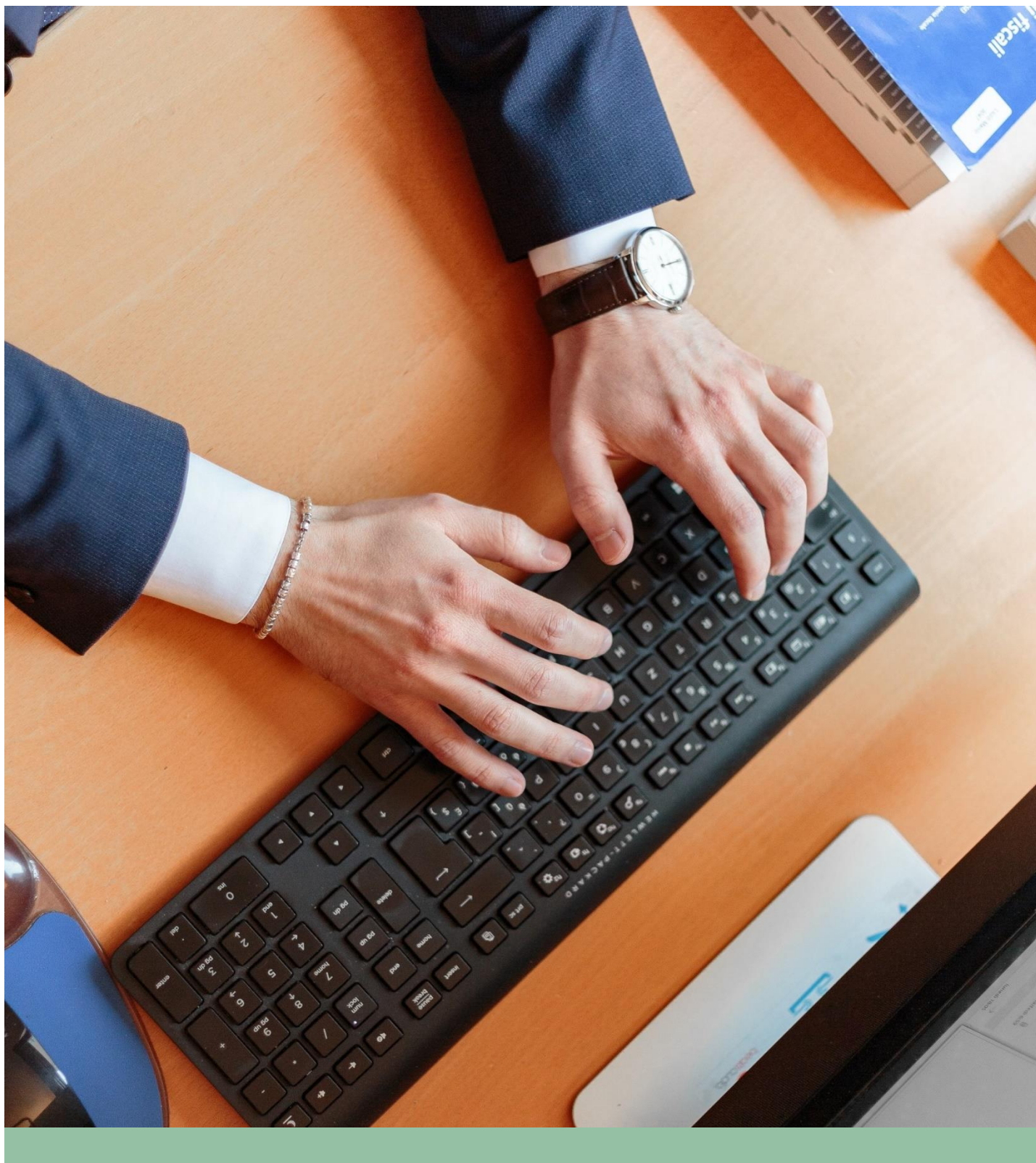





# INFORMATION GOVERNANCE WORK PROGRAMME 2020/21

Date: 27 July 2021

ANNEX 3



## CONTENTS

 Purpose of the report <b>3</b>	 UK GDPR action plan update <b>3</b>
 Covid-19 pandemic <b>4</b>	 Training <b>5</b>
 Information security incidents <b>5</b>	 Subject access requests – internal reviews <b>5</b>
 Data protection impact assessments <b>5</b>	 Surveillance <b>6</b>
 Law enforcement <b>6</b>	



**Kirsty Bewick**  
Information Governance Manager



**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 Head of Business Development and Improvement and provides overall direction and guidance on all information governance matters. CIGG also helps to support the Council's Senior Information Risk Owner (SIRO) to discharge her 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 2020/21 action plan was reported to CIGG throughout the year. The action plan was updated as work was completed. A number of actions were identified as undeliverable during the year due to the impact of the Covid-19 pandemic on the Council. The decision was therefore made to defer these to the 2021/22 action plan. A new 2021/22 action plan has now been provided to the Council. This includes a detailed breakdown of actions required to achieve agreed deliverables.
- 7 A review of the Council's existing privacy notices was completed. The review identified a number of privacy notices which require updating or preparing. This will be done in conjunction with the review of the Council's Information Asset Register (IAR) which is taking place in 2021/22.



- 8 A number of new privacy notices were also progressed including those for Democratic Services and HR. Advice was given and amendments were made to other privacy notices throughout the year, as issues arose.
- 9 The Information Governance Policy framework was presented to CIGG in January 2021. Following this, the information security incident handling policy was published. The remaining policies are due to be published shortly.
- 10 A Special Category policy, required to satisfy Schedule 1, Part 4 of the Data Protection Act 2018, was presented to CIGG in January 2021. The policy was subsequently approved by CIGG in April 2021. This document lists the types of special category information the Council processes and their lawful basis to do so. The policy has now been published.
- 11 The Information Asset Register (IAR) was amended to reflect UK GDPR compliance needs and now includes columns for law enforcement processing. Outstanding IAR work was completed by HR with Veritau's support. A number of areas requiring limited amendments were actioned as part of other projects. Major outstanding areas include Legal, Housing and Environmental Health.
- 12 A gap analysis of the Council's Information Sharing Agreements (ISAs) was completed and a number of areas of concern identified. The areas to prioritise for immediate action have been agreed. Work is ongoing to establish what other ISAs and data processing contracts are held, or to obtain the relevant contracts. Actions to address gaps identified are included in the 2021/22 action plan.



## COVID-19 PANDEMIC

- 13 As a result of the Covid-19 pandemic, Veritau produced a number of documents to support the Council to meet its UK GDPR and Data Protection obligations.
- 14 The Council worked with other members of the North Yorkshire Information Sharing Protocol group to put in place an overall Information Sharing Agreement (ISA) for Covid-19 related information sharing. A number of specific privacy notices were prepared and published, and the main Covid-19 privacy notice was also amended to include elements of Track & Trace processing.
- 15 A range of guidance documents was also provided to advise staff on secure home working, sharing employee personal data and the Council's obligations around statutory requests. Other ad-hoc advice was also given as required.



## TRAINING

- 16 It was agreed at CIGG that training sessions will now be held online and in smaller groups. The training sessions to be delivered include Records Management, Data Protection Rights and Principles and a new session around Data Protection Impact Assessments. No sessions were held in 2020/21 due to the impact of the Covid-19 pandemic, but training will recommence as part of the 2021/22 action plan.



## INFORMATION SECURITY INCIDENTS (DATA BREACHES)

- 17 Information Security Incidents have been reported to Veritau as required. The incidents are assessed, given a RAG rating and then investigated as required. Green incidents are unlikely to result in harm but indicate a breach of procedure or policy; Amber incidents represent actual disclosure, but harm is unlikely to be serious; and Red incidents are sufficiently serious to be considered for self-reporting to the 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).
- 18 The number of Security Incidents reported to the Council and Veritau in 2020/21 are as follows:

Year	Quarter	Red	Amber	Green	White	Total
2020/21	Q1	0	2	2	1	5
	Q2	0	1	0	2	3
	Q3	0	1	2	0	3
	Q4	0	2	4	1	7
	Total	0	6	8	4	18

- 19 A new information security incident process was approved by CIGG in June 2021. The new process will be used for all future incidents.



## SUBJECT ACCESS REQUESTS - INTERNAL REVIEWS

- 20 Veritau provides advice on internal reviews relating to Subject Access Requests as required.



## DATA PROTECTION IMPACT ASSESSMENTS

- 21 Veritau supported the Council in completing a number of DPIAs in 2020/21 as well as providing advice on whether a DPIA was required for other projects.

- 22 DPIAs completed include Pick Protect and Reform Canvass work. Advice on DPIAs has also been given for recording meetings and using biometric data.
- 23 A number of DPIAs are in progress which Veritau will continue to support. These include MyView and the Heritage Action Zone project. Following on from the Surveillance project (see below), a number of new DPIAs have been identified and will be progressed in 2021/22.

## SURVEILLANCE

- 24 In early 2020/21, Veritau had a number of meetings with the Head of Communities, Partnerships and Customers (the designated Senior Responsible Officer with the Surveillance Camera Commissioner) and others to progress work on overt surveillance activities. The surveillance log was circulated and a gap analysis completed. This included the need to ensure all relevant DPIA's and ISAs were in place. This work is now complete.
- 25 Draft policy documents and privacy notices are also complete, and have been presented at CIGG for consultation.
- 26 Discussions also took place on other aspects of surveillance, including covert surveillance. To assist with this, Veritau conducted a review of the current RIPA (Regulation of Investigatory Powers Act) policy and provided general advice. The policy is currently being reviewed by Council officers. It has been agreed that all surveillance documentation will be presented to the Audit & Governance Committee for consideration once the documentation has been finalised.
- 27 Veritau has also supported the Council to collate relevant information for the Surveillance Camera Commissioner.

## LAW ENFORCEMENT

- 28 An initial scoping exercise has been 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 reflect where law enforcement processing is taking place, linking back to the relevant legislation and/or enforcement policies.
- 29 Documents such as the new DPIA template and guidance were also drafted to include law enforcement considerations.
- 30 Privacy notices were reviewed with law enforcement in mind. It has been agreed that any changes to the notices will occur at the same time as any identified updates as noted in paragraph 7 above. The corporate privacy notice has been updated to include information about conditions for criminal offence data, enforcement investigations and prosecutions.
- 31 The Law Enforcement Policy, required for compliance with section 42 of the Data Protection Act 2018 to cover data processed under Part 3 of the Act

alone, was approved by CIGG in April 2021. The policy has now been published.

- 32 A virtual training course has also been designed although further work is being carried out to ensure that the course meets all the requirements of the Council. The intention is to make the course available later in 2021.