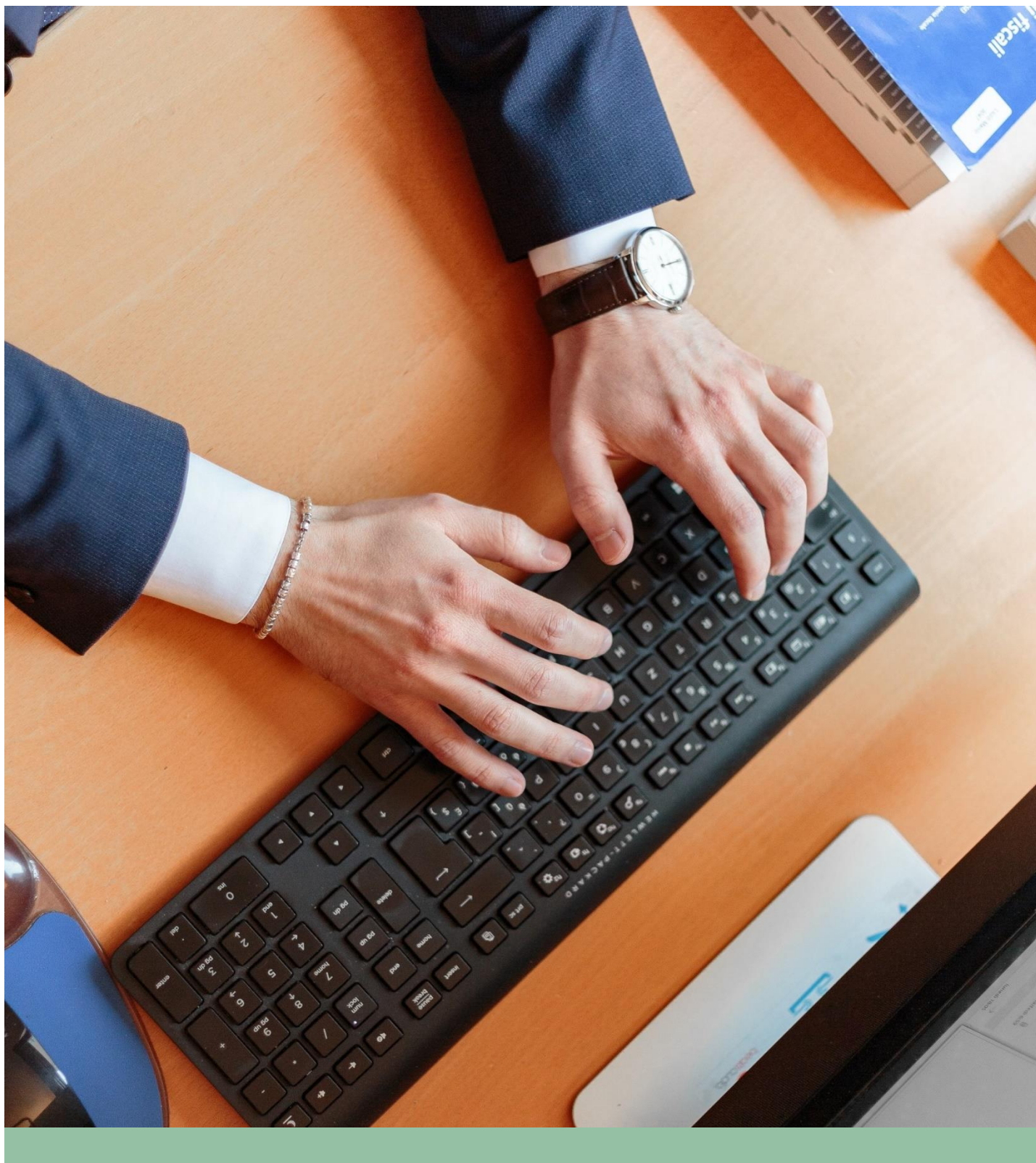


# INFORMATION GOVERNANCE WORK PROGRAMME 2021/22

Date: 26 January 2022

ANNEX 3



## 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
- 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, who is the Senior Information Risk owner for the Council (SIRO) and provides overall direction and guidance on all information governance matters. CIGG also helps to support the (SIRO) to discharge their responsibilities. CIGG is currently coordinating the delivery of the Council's UK GDPR action plan, which includes reviewing and updating the Council's Information Sharing Agreements (ISAs) and Data Processing Contracts (DPCs).

## UK GDPR ACTION PLAN UPDATE

- 6 A new 2021/22 action plan has been provided to the Council. This includes a detailed breakdown of actions required to achieve and maintain compliance with Data Protection laws. Work is ongoing to ensure that this action plan is updated regularly.
- 7 Following completion of the privacy notice review in 2020/21, Veritau are in the process of applying the relevant changes to the privacy notices. So far, 24 notices have been reviewed and have been sent to service areas for their comments and updates. Once this work is completed, the updated privacy notices will be published.
- 8 The amended Information Governance Policies have been approved and have been published.

- 9 The Information Asset Register (IAR) was amended to reflect UK GDPR compliance needs and now includes columns for law enforcement processing. A review of the IAR is ongoing with copies being sent to each service area for them to check. Currently, the main areas which require further work are Housing and Environmental Health. Veritau are in contact with these areas and are working with them to ensure their IAR entries are correct.
- 10 In 2020/21 a gap analysis of the Council's ISAs and DPCs was completed and a number of areas were identified where there was insufficient information. Work is ongoing to locate and acquire copies of documentation in these areas so they can be reviewed and updated with the appropriate clauses where necessary. Where documentation has been received, this has been reviewed.

## TRAINING

- 11 It was agreed at CIGG that training sessions will be held online and in smaller sessions. The training sessions, which will be bookable, include Records Management, Data Protection Rights and Principles and a new session around Data Protection Impact Assessments. The Council has been approached in relation to identifying dates and once these are confirmed, the sessions will be formally booked in.

## INFORMATION SECURITY INCIDENTS (DATA BREACHES)

- 12 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 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).
- 13 The number of Security Incidents reported in 2021/22 up until the end of December are as follows:

Year	Quarter	Red	Amber	Green	White	Total
2021/22	Q1	1	0	4	1	6
	Q2	0	0	2	1	1
	Q3	0	0	0	0	0
	Q4					
	Total	1	0	6	2	7

- 14 The red incident in Q1 was reported to the ICO who responded with no further actions for the Council.

## **SUBJECT ACCESS REQUESTS - INTERNAL REVIEWS**

- 15 Veritau provides advice on internal reviews relating to Subject Access Requests as required. Going forward, Veritau will be providing further assistance to the Council with all aspects of subject access requests. Future reports to the committee will therefore reflect this.

## **DATA PROTECTION IMPACT ASSESSMENTS**

- 16 Veritau is supporting the Council in completing a number of DPIAs as well as providing advice on whether a DPIA is required for other projects.
- 17 CCTV for Town Centre: An initial draft is being prepared to cover town centre CCTV cameras. The relationship the Council has with the police will need to be explored as part of this work as only the police access the footage for law enforcement purposes.
- 18 MyView: In 2019, the council implemented MyView. However, a DPIA was not done before implementation. A first draft of the DPIA was received by Veritau in September 2020. Comments were returned to the service area at that time and the matter has been discussed in CIGG, most recently in December 2021 where it was agreed that the Council would follow this up and ensure that the DPIA was completed.
- 19 ONS Data Sharing: An initial draft is being prepared to cover the sharing with ONS. This has been an ongoing project with both Veritau and the Council's legal services involved to ensure that the sharing of information is lawful. ONS has provided numerous pieces of information which has included confirming that the purpose for the data was in line with their statutory functions.
- 20 A number of DPIAs have been identified as needing to be completed following the completion of the surveillance review (see below). These will be progressed during 2021/22.

## **SURVEILLANCE**

- 21 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.
- 22 Policy documents and privacy notices have been approved and have been published.

## LAW ENFORCEMENT

- 23 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.
- 24 Documents such as the new DPIA template and guidance were also drafted to include law enforcement considerations.
- 25 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.
- 26 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.
- 27 A virtual training course which has been designed to meet the requirements of the Council is now available. Selected officers will now have the opportunity book onto this course.