AUDIT COMMITTEE **22 MARCH 2022**

SUBJECT:	**INFORMATION GOVERNANCE UPDATE**
DIRECTORATE:	**CHIEF EXECUTIVE AND TOWN CLERK**
REPORT AUTHOR:	**SALLY BROOKS, DATA PROTECTION OFFICER (DPO)**

1. Purpose of report

1.1. To update committee on Information Governance management. This includes monitoring of the council's compliance with data protection legislation including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

2. Background of reporting

2.1. Reports are submitted on a bi-annual basis the last report being provided to committee in September 2021.

3. Information governance risk register

3.1 Attached at Appendix A (Part B) is the updated Information Governance risk register. The following risks are highlighted for comment:

4 Training

4.1 Data protection training is a legal requirement. The Information Commissioner's Office (UK regulator) recommends it is renewed every 2 years and preferably annually for an organisation such as the council. The council have agreed to renew training annually for all staff and to provide training for all staff on induction.

4.2 The council have obtained new e-learning provided by an external provider. The training is accredited by the National Cyber Security Centre (NCSC) and covers both data protection training and cyber security training.

4.3 The need for cyber security training is essential given the increase in staff remote working and cyber activity. The risk of cyber activity is currently particularly concerning considering recent events in Ukraine. The NCSC have warned the council and other organisations that the UK's cyber risk has heightened following a string of cyber-attacks targeting Ukraine's digital infrastructure. They state that recently they have seen the EU mobilise a team of cyber security experts to help Ukraine fight off cyber-attacks from Russia and as the situation continues to escalate, they can see cyber-attacks that have international consequences. In this light, the NCSC has urged organisations to strengthen cyber security posture.

4.4 The e-learning for all staff and councillors includes topics such as data protection, data handling, password security, appropriate use of social media,

phishing emails and how to identify/report cyber security risks and suspicious cyber activity.

4.5 The training also includes a higher-level training package for Information Asset Owners (IAO's) 'Data Confident' and a bespoke training package for Councillors who have responsibility for data protection as 'Controllers' in their own right, when processing constituents' personal data.

4.6 The e-learning along with completion of the low-risk forms for relevant staff (without access to the network) was rolled out December 2021 and the deadline for completion, the end of January 2022, has now passed. From recent reports around 68% of all staff and councillors have now completed the training, with feedback on the course content being extremely positive. Non-completers are currently being chased from training reports to complete.

4.7 IAO's are required to complete their annual IAO Checklist online by the end of April 2022. The checklist requires them to assess all information assets held in their area by checking that the corporate Information Asset Register is up to date, Information Sharing Agreements and Contracts are data protection compliant and personal data is being disposed of in accordance with our Retention & Disposal Schedules.

4.8 This year completion of the IAO Checklist is particularly important as any additional datasets created in response to the Covid pandemic need to be considered carefully. IAO's are given the opportunity to meet with the Data Protection Officer to discuss their Checklists and any outstanding actions and all results are ultimately shared, as required, with our Senior Information Risk Officer.

5. ICT Security Policies

5.1 Previously the ICT Security policies was a red risk on the Information Governance risk register as these were due for renewal. This is no longer a red risk as the ICT Security policies have now been updated and were approved by Executive Committee on the 21 February 2022.

5.2 The new ICT Security policies will now be promoted with staff and councillors through bite sized communications and will be available to all through the council's policy management software NET-consent.

6. Management of documents in Office 365

6.1 Full use of the Office 365 suite including Microsoft Teams and SharePoint continues to be rolled out to staff.

6.2 Office 365 has the potential to improve information management in terms of available tools in retention, security, data leakage and access control as well as compliance with information requests such as Freedom of Information and Subject Access Requests.

6.3 The Information Governance working group have been considering these tools and in particular retention and management of documents in Office 365.

Proposals have been drafted and are currently being considered by CMT. It is essential that retention in Office 365 is implemented from the outset and that existing data held is reviewed and deleted where possible. This is to ensure the council does not retain personal data longer than necessary which is a fundamental principle of data protection and key to business efficiency.

7. Annual Governance Statement (AGS)

7.1 The AGS status for Information Governance was downgraded from Red to Amber due to progress made in the implementation of the GDPR. IG has since been removed from the AGS although remains closely monitored with reports being submitted to IG Board CLT, CMT as and when required and Audit Committee.

8. Strategic Priorities

8.1 This work ensures that staff are high performing in their collection and processing of customer's data. It also assists to ensure that the council is trusted to deliver the services and ensures compliance.

9. Organisational Impacts

9.1 Finance (including whole life costs where applicable)

There are no financial implications arising from this report, as the resources will come from existing budgets.

9.2 Legal Implications including Procurement Rules

There are no legal implications arising out of this report.

9.3 Equality, Diversity and Human Rights

The Public Sector Equality Duty means that the Council must consider all individuals when carrying out their day-to-day work, in shaping policy, delivering services and in relation to their own employees.
It requires that public bodies have due regard to the need to:

- Eliminate discrimination
- Advance equality of opportunity
- Foster good relations between different people when carrying out their activities

There is no impact arising from this report regarding these issues.

10. Risk Implications

10.1 The council must comply with data protection legislation. Non-compliance may result in enforced external audits, enforcement notices, monetary fines, criminal prosecutions of individual's, compensation claims and loss of public/partner trust.

11. Recommendation

11.1 To note the content of the report and provide any comment.

Is this a key decision?	No
Do the exempt information categories apply?	No
Does Rule 15 of the Scrutiny Procedure Rules (call-in and urgency) apply?	No
How many appendices does the report contain?	1
List of Background Papers:	None
Lead Officer:	Data Protection Officer, Sally Brooks