By:	Ben Watts, General Counsel (Senior Information Risk Owner)
To:	Policy and Resources Cabinet Committee – 16th March 2018
Subject:	**SENIOR INFORMATION RISK OWNER UPDATE**
Classification:	Unrestricted

Summary: This report provides an update regarding the implementation of forthcoming Data Protection legislation

Introduction

1. The Senior Information Risk Owner (SIRO) is the officer responsible across the whole Council for Information Governance. The SIRO is responsible for the strategy, acts as an advocate for good practice in Information Governance at CMT and is required to provide a statement of assurance as part of the Council's Annual Governance Statement. Ben Watts is Kent County Council's SIRO.
2. Information governance means the effective management of information in all its forms and locations. It encompasses efficient ways of handling information, robust management of the risks involved in the handling of information, and compliance with regulatory and statutory guidance including Data Protection and Freedom of Information.
3. Information governance is about electronic and paper based information, about how it is held, used and shared. The importance of good information governance has been highlighted by the Information Commissioner and the Permanent Secretary for the Department for Communities and Local Government. Members of this Committee will have read the stories of significant fines faced by other public sector bodies for failures to manage information properly.
4. Information governance is also concerned with keeping information safe and secure and ensuring it is appropriately shared when necessary to do so. This is a significant challenge for all organisations but particularly so for large complex public sector organisations such as KCC dealing with a wide range of functions.
5. Issues and updates relating to information governance are reported to Policy and Resources Cabinet Committee and Governance and Audit Committee as appropriate.

The General Data Protection Regulation (GDPR)

6. Members have previously been advised of the forthcoming General Data Protection Regulation (GDPR) which is intended to strengthen and unify data protection for individuals and will become applicable to Kent County Council and Members from 25th May 2018. It heightens the standards required as well as imposing new obligations.

7. Among the regulations, there are changes to the potential legal justifications for processing data, significant changes to the requirements for consent, heightened requirements for privacy notices and increased rights for data subjects.

8. GDPR will require various modifications to how the council processes data across the organisation and with our partners, providers and members of the public and work is already underway across directorates to facilitate this. In recent months, the ICO has been providing helpful guidance and clarity in relation to GDPR that we have been reflecting in our planning.

9. The regulations allow for the ICO to impose administrative fines up to a maximum of 20 million Euros (approx. £18m) for infringements. The ICO, in recent months, have made it clear that they intend to proportionately regulate notwithstanding their new and increased powers.

10. To prepare for the legislation, officers across the council have been looking at the readiness of directorates for the necessary changes. A number of discussions have taken place at CMT and in the autumn, Corporate Directors nominated officers who have been taking the lead for their directorate in developing readiness for GDPR.

11. We are currently amending and changing the council's policies in the light of guidance now received from the ICO and these will all be in place in the coming weeks.

12. It must be remembered that the organisation has not allocated additional resource to deliver this significant change and officers are delivering in addition to their "day jobs". Similarly, some of the regulation is predicated without an understanding or reflection on the type and nature of some of the historic data that KCC holds.

13. It has been agreed that the council would adopt a proportionate response to compliance with GDPR and this will mean that work will continue past the implementation date. As part of our learning culture, we will continue to reflect on decisions by the ICO and develop and amend our policies as the regulation begins to be enforced.

14. Staff from Governance and Law have worked in conjunction with the Internal Communications team to raise awareness in relation to GDPR through updates to KNet and the development of a communications strategy. This has

included the presentation of key issues on TV screens in KCC buildings to build knowledge and awareness.

15. Further updating of staff and Members will be taking place over the next 12 weeks with weekly updates on the necessary steps and preparation ahead of May.

16. Members received initial training on information governance and data protection as part of their induction sessions after the election in May. Given the impact of the new regulations on Members individually, training on the GDPR will be provided in the period up to May 2018. The next stage of this training was an overview of GDPR and the repercussions of this new legislation on Members and for the County Council which took place on 2nd November 2017. Further training is being arranged immediately after the Easter recess.

17. Implementation of GDPR is in the intensive phase and the corporate risk register has been adjusted accordingly. The SIRO is supported by a range of talented officers across the organisation and the project is being led by Lauren McCann, Principal Solicitor. Corporate Management Team, individual Corporate Directors and Directorate Management Teams continue to receive regular strategic updates from the SIRO and Project Manager.

18. An officer working group was established in the autumn with representation from across the organisation and has been meeting fortnightly to work through the project plan to follow and implement the ICO guidance notes and to achieve readiness. Intensive work continues and the hard work and support of all officers is appreciated.

19. Officers from KCC are supporting colleagues across the county in the renegotiation of the Information Sharing Agreement that underpins much of the multi-agency work in Kent and which is being refreshed ahead of May.

20. GDPR requires organisations such as Kent to appoint a Data Protection Officer. This role The DPO's minimum tasks are defined in Article 39:

    a. To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
    b. To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
    c. To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

21. Given the overlap between the responsibilities of the General Counsel role and statutory Monitoring Officer and the fact it replaces most of the current SIRO role, it is proposed that this be added to the General Counsel role profile. Formal steps around this proposal will be taken through relevant committees ahead of May.

Update on Information Governance Training

22. Members of this committee will be aware that officers are required on a mandatory basis to complete training on Data Protection and Information Governance. This mandatory training requirement has been extended to include GDPR and all officers will be required to undertake the training.

23. Given the enhanced obligations placed on KCC by GDPR, it is the view of the Monitoring Officer that consideration should be given to Members also being required to complete the training that is mandatory for staff.

24. The training is an online and interactive course that can be undertaken via the KCC intranet.

25. Ahead of further discussions at Selection and Member Services Committee and County Council, Members of this committee are asked to comment on the suggestion that Members be required to complete the training.

Recommendations

26. It is recommended that Members **NOTE** the report and **COMMENT** on the suggestion that Members should also be required to complete the mandatory information governance, data protection and GDPR training.