AUDIT COMMITTEE
20 DECEMBER 2017

ITEM NO. .....5.....

GENERAL DATA PROTECTION REGULATIONS (GDPR) COMPLIANCE PROGRAMME

SUMMARY REPORT

Purpose of the Report

1. To provide Audit Committee with an overview of the General Data Protection Regulations (GDPR) and the Council's progress to date in preparing for implementation.

Background

2. The UK will remain a member of the European Union on 25 May 2018 at which time the GDPR will replace the Data Protection Act (DPA) 1998, without the need for implementing national legislation. The GDPR will remain in place until the UK leaves the EU or implements primary legislation.

3. The UK Government is currently considering the Data Protection Bill which will update the UK's data protection laws for the digital age. The Bill was introduced to the House of Lords on 13 September 2017.

4. The Data Protection Bill will need to mirror the GDPR in order to prevent UK being considered an 'inadequate' country for data protection purposes; preventing our ability to trade with EU member states.

5. The GDPR build upon the DPA and as such the work the Council has done to date provides a solid foundation for achieving GDPR compliance.

Overview of the General Data Protection Regulations

6. The GDPR updates the definition of personal data to include an identification number, location data and on-line identifiers such as IP addresses. It also extends the definition of special categories of personal data (formerly sensitive personal data) to include genetic data and biometric data where that data is processed to uniquely identify an individual, for example, iris scanning technology used for a door entry systems.

7. In addition the GDPR updates the principles relating to the processing of personal data, which may be summarised as:

(a) Lawful, fair and transparent;
(b) Purpose limitation;
(c) Data minimisation
(d) Accuracy;
(e) Storage limitation;
(f) Integrity and confidentiality.

8. The GDPR also introduces an accountability principle which underpins all of the above and requires the data controller i.e. the Council to be able to demonstrate compliance. In order to demonstrate accountability the Council will need to place greater emphasis on the documentation it keeps regarding the processing of personal data.

9. The GDPR introduces a new liability for data processors i.e. organisations processing personal data on our behalf, for example, care homes and the confidential waste disposal contractor where they act in a manner contrary to what is detailed in the written agreement or contract.

10. The GDPR requires the Council to appoint a Data Protection Officer (DPO) who shall have at least the following tasks:

(a) To inform and advise the Council and the employees of their obligations to comply with the GDPR and other data protection laws;
(b) To monitor compliance with the GDPR, other data protection provisions and Council policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations and related audits;
(c) To provide advice on data protection impact assessments and monitor impact assessment performance; and
(d) To cooperate with and act as a first point of contact for the ICO.

The Data Protection Officer will also be the first point of contact for the general public in relation to data protection issues.

11. The GDPR makes privacy by design a legal requirement and the completion of Data Protection Impact Assessments mandatory in situations where processing data is likely to result in high risk for individuals, for example, where new technology is being deployed; a profiling operation is likely to significantly affect individuals; or where the Council is undertaking large scale processing of special category data.

12. The GDPR enhances existing rights under the DPA and introduces new rights for individuals (data subjects) which include:

(a) Right to be informed (what we must tell you);
(b) Right of access (to get a copy of your personal data);
(c) Right to rectification;
(d) Right to erasure ('right to be forgotten');

(e) Right to restriction of processing;
(f) Right to data portability;
(g) Right to object;
(h) Right not to be subject to automated decision making;
(i) Right to complaint to the ICO;
(j) Right to effective judicial remedy.

13. The GDPR introduces a requirement to report data breaches to the ICO within 72 hours, where the breach is likely to result in a risk to the rights and freedoms of the individuals affected. Where the data breach is likely to pose a high risk to the rights and freedoms of the data subject(s) in most cases we will also have to notify those individuals affected.

14. The GDPR also introduces tougher monetary penalties i.e. fines of up to €20,000,000 or 4% of annual worldwide turnover, whichever is greater.

Progress to date

15. The ICO's guide Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now details the steps organisations should be taking in preparation for the implementation of GDPR on 25 May 2018.

16. In addition to considering what the Council needs to do in order to implement the ICO's 12 steps, the DPO is currently assessing the Council's position as part of the GDPR compliance programme.

17. Details of the areas of work identified and the Council's position/progress to date is detailed in the table at Appendix 1.

Recommendations

18. That Audit Committee notes the content of the attached report and the progress made to date in preparing for the implementation of GDPR.

APPENDIX 1

What	Who	When	Status
Audit To assist Council as data controller in demonstrating compliance (accountability).			
Internal Audit	Internal Audit	Post 25/05/2018	DPO discussed with Audit Manager
Agree scope of audit	DPO	25/05/2018	Draft questions written
Awareness Make sure that decision makers and key people are aware that the law is changing and appreciate the impact this is likely to have.			
Briefing, loo news, screens in collaboration	DPO	30/09/2017	
SMTs and Team meetings	DPO	25/05/2018	Ongoing
Report to COE, COE, SIGG	DPO	31/10/2017	
SMN Session	DPO	31/01/2018	
Update AC10 course	DPO	25/05/2018	
CCTV Ensure CCTV is reviewed on an annual basis and has regard to advice of Surveillance Camera Commissioner and reasonable expectation of privacy.			
CCTV	DPO/CCTV & Parking Enforcement Manager	01/04/2017	
Refuse Vehicle	DPO/Head of Environmental Services	01/04/2017	
Body Worn Video	DPO/Head of Environmental Services	01/04/2017	
Signage/privacy notices	DPO/ CCTV & Parking Enforcement Manager/ Head of Environmental	01/04/2017	

What	Who	When	Status
	Services		
Children Ensure enhanced rights for children detailed in GDPR are met.			
Consider whether we need systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity	DPO	01/03/2017	
Compile a list of on-line services the Council provides to children	DPO	01/03/2017	
Consent Establish where we rely on consent at present, consider whether there are more appropriate conditions for processing on which we can rely. Where it is necessary to obtain consent refresh to ensure it meets the requirement on the GDPR.			
Clarify condition for processing personal / special categories of personal data	Service areas with support from DPO		To be done as part of review of privacy notices
Contracts Revise contracts in light of Articles 28 and 29 to ensure compliance and transfer liabilities to data processors as appropriate.			
Issue advice on GDPR compliance to contracts	DPO	31/09/2017	Draft advice produced.
Share good practice from Regional IG forum with contracts	DPO	Ongoing	
Alert contracts to any standard clauses adopted by the Commission or ICO	DPO	Ongoing	ICO consultation on contract and liabilities between controller and processors to close 10 Oct 2017
Data Breaches Ensure Council has appropriate procedures in place to manage information security incidents, including data breaches.			
Revisit Information	Information	30/10/2017	

What	Who	When	Status
Security Incident Procedure	Security Manager		
Data Flow Mapping Map data flows in and out of organisation.			
To be done with individual services as part of review of privacy notice/IAR/ISAs	Service areas with support from DPO	Ongoing	Data flows detailed in existing ISAs
Data Protection by Design Ensure data protection is considered at the conception of new projects.			
Embed GDPR into project management process	DPO	31/01/2018	
Embed into ICT procurement documentation	Information Security Manager	Done	
Add to front cover of committee reports	DPO	01/04/2018	
Agree a DPA Impact Assessment Tool	DPO	30/11/2017	
Data Protection Officer			
Designate a suitably qualified Data Protection Officer (DPO)	Complaints & Information Governance Manager	01/04/2017	Designated as DPO. Existing knowledge of DPA Completed Act Now GDPR Practitioner Certificate
DPO must have direct reporting line to highest level of senior management	Senior Information and Risk Owner (SIRO)	01/04/2017	Reports to SIGG chaired by SIRO (documented in Information Governance Framework) Supports Caldicott Guardian (documented in Caldicott Function Diagram) SIRO is DPO's

What	Who	When	Status
			Director Access to COE on ad hoc basis
Resources required – time, financial resources, infrastructure (premises, facilities, equipment) and staff	DPO	Ongoing	DPO forms part of existing role. Supported by Information Governance Officer as part of existing role
Individual Rights Check procedures to ensure they cover all the rights individuals have, including deleting personal data or providing data electronically and in a commonly used format.			
Update SAR Procedure	DPO	25/05/2018	
Consider producing Corporate 'Information Rights Procedure'	DPO	25/05/2018	Draft written
Establish and document service specific rights – privacy notice	DPO	25/05/2018	
Information Sharing Agreements (ISAs)			
Review existing ISAs	Service areas with support from DPO	31/01/2018	
ISAs need implementing in those areas that do not currently have one	Service areas with support from DPO	31/01/2018	DPO to issue advice to all services who process personal data
Develop central record of ISAs	DPO	Ongoing	
Information we hold (Information Asset Register/Privacy Notices) Need to maintain records of processing activities - document the personal data held, where it came from and who it is shared with, etc. Review current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. Organise information audits where necessary.			
Agree Corporate Information Asset Register (IAR) Template	SIGG	16/11/2017	Agreed at SIGG
Rolled out across Council	DPO	17/11/2017	Done

What	Who	When	Status
Review existing privacy notices on web	Service areas with support from DPO	31/01/2018	Updated in light of GDPR – DPO to check compliance
Privacy notices need implementing in those areas that do not currently have one	Service areas with support from DPO	28/05/2018	DPO to issue advice to all services who process personal data
Joint Controllers Identify any joint data controllers in order to comply with Article 26 of GDPR.			
To be done with individual services as part of review of privacy notice/IAR/ISAs	Service areas with support from DPO	Ongoing	