AUDIT COMMITTEE – 4TH SEPTEMBER 2018

Report of the Head of Customer Experience

Part A

ITEM 05 UPDATE ON THE GENERAL DATA PROTECTION REGULATION (GDPR)

Purpose of Report

The purpose of this report is to provide the Committee with an update on the progress the Council have made following the introduction of the new General Data Protection Regulation (GDPR).

Recommendation

That the Committee note the report.

Reason

To provide the Committee with the Council's current position in complying with the General Data Protection Requirements.

Policy Justification and Previous Decisions

The General Data Protection Regulation came into effect on the 25th May 2018. This constituted the biggest change in data protection rules in two decades. The Data Protection Act 2018 also came into force in the United Kingdom on the 25th May 2018

Report Implications

The following implications have been identified for this report.

Financial Implications

None.

Risk Management

There are no specific risks associated with this decision.

Background Papers:

Officers to contact: Karey Barnshaw (01509 634923)
karey.barnshaw@charnwood.gov.uk

Megan Bilton (01509 634711)
megan.bilton@charnwood.gov.uk

Part B

Background

1. The General Data Protection Regulation (GDPR) came into force on 25th May 2018 and is intended to strengthen and unify data protection for all individuals within the European Union (EU).

   The GDPR applies to the processing of personal data carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

2. In addition to the GDPR, the updated Data Protection Act 2018 also came into force in the UK on 25th May. The Act applies the GDPR standard, sets out the UK specific elements (such as exemptions to the GDPR) and also covers the EU Crime Directive.

3. The GDPR brought with it more rights for Data Subjects[1], additional duties for Data Controllers[2] and increased powers for the Independent Supervisory Authority[3], including the ability to fine organisations up to £17m.

4. In June 2017 the Council appointed a Data Protection and Information Security Officer to begin preparations for compliance with the GDPR and to be the mandatory Data Protection Officer required under the new legislation.

5. In August 2017 the Council began working through a project plan listing key activities to ensure readiness for the commencement of the GDPR.

   The project plan (see Appendix A) covers 9 areas, in line with guidance from the Information Commissioner's Office:
   - Awareness
   - Information held
   - Privacy information
   - Individual's rights
   - Consent
   - Children
   - Data breaches
   - Data Protection by Design and Default and Impact assessments
   - Contracts

[1] Data Subject – identifiable natural person data relates to
[2] Data Controller – organisation which determines the purpose and means of processing
[3] Independent Supervisory Authority – in England and Wales this is the Information Commissioners Office

Current Position

6. Regular GDPR updates have been provided to the Council's Senior and Corporate Management Teams in respect of progress with the project plan and to inform them of actions required to be taken by services. As at July 2018, two areas remain outstanding for completion.

   The first is the Record of Processing Activity which is a requirement of the GDPR. Although the Council has a corporate document covering all service areas work remains ongoing with services to ensure that all entries are accurate and applicable to the work carried out at Charnwood.

   The second is ensuring that all relevant contracts we hold are updated to include the clauses required to provide GDPR compliance. Work was undertaken to notify contractors of this requirement and to gain their assurance that they will be able to meet their GDPR obligations. The work to update contracts now sits with Legal Services.

7. There are other activities which the Council needs to undertake, to ensure compliance, however these are wider corporate actions rather than specific to GDPR.

   GDPR requires that information is not held for longer than is necessary. Discussions with services have revealed that some of our legacy IT systems do not easily allow the removal of data, and therefore data is being held indefinitely. In order to comply with this requirement, services need to review their document management processes, assess how long data is required and ensure that they proactively delete information past this deadline.

   Another action which is underway is to centrally record and review Information Sharing Agreements which the Council are party to. This will allow a corporate overview of which organisations the Council may share data with, ensure that Data Subjects are aware of this and allow the Council to comply with the requirements of each agreement.

8. The Audit and Risk Team completed an internal audit of Data Protection and Information Security in July 2018 which provided an assurance rating of Substantial. The detail of this report is provided to the Committee within Item 06 of this Agenda.

9. It is acknowledged that processes and procedures may need to change as rulings and case law start to come out in relation to the GDPR, or as new best practise guidance is shared.

   The Council has already shown flexibility in this regard, for example; in its approach following customer feedback regarding the automated privacy message attached to phones.

10. The Council has acknowledged that the 25th May 2018 was not an end date to ensure compliance; rather that it is an ongoing requirement.

    The Data Protection Officer will ensure that documents and processes are reviewed regularly, manage the staff training which is to be completed annually and be the first point of contact both internally and externally for all matters relating to Data Protection.

Appendices:

Appendix A - GDPR Project Plan

GDPR Plan – Position as at August 2018

Title:		GDPR		**Date:**	August 2017 Last update August 2018
Objective:		Implement changes in preparation of the GDPR			
TASK		**LEAD**	**START DATE**	**END DATE**	**UPDATE**
1. Awareness					
1.1	Introduce DPO to Officers – One Charnwood article				
	1.1.1 Raise key issues with SMT and keep them updated	SJ	6 Sept 17	Ongoing	COMPLETED
	1.1.2 Raise key issues with CMT and keep them updated		7 Sept 17	Ongoing	COMPLETED
	1.1.3 Speak to different services where impacts are highest	MB	1/10/17	1/2/18	COMPLETED
	1.1.4 Keep officers up to date with changes being introduced	SJ	1/10/17	1/4/18	COMPLETED
	1.1.5 Keep Mbrs up to date with changes being introduced	SJ / AW	7 Sept 17	Ongoing	COMPLETED
	1.1.6 Intranet site	MB	1/6/17	1/10/17	COMPLETED
	1.1.7 Internet site	MB	1/6/17	1/8/17	COMPLETED
1.2	Mandatory e-learning				
	1.2.1 Identify which staff will need to undertake the training	MB	1/9/17	1/10/17	COMPLETED
	1.2.2 Inform officers that e-learning is live, and set out timescales for completing	SJ	1/10/17	Ongoing	COMPLETED
	1.2.3 Set up reporting, so we can log completion, and chase those who have not completed within timescale	Lyn Smith	1/10/17	Ongoing	COMPLETED
1.3	F2F training				
	1.3.1 Identify services, where specific training is required	MB	1/12/17	1/2/18	COMPLETED.
	1.3.2 Identify whether training can be delivered in house, or requires external trainer		1/1/18	1/2/18	COMPLETED
	1.3.3 Provide training for members		1/1/18	1/4/18	COMPLETED

	TASK		LEAD	START DATE	END DATE	UPDATE
1.4	Governance					
	1.4.1	Check policy and procedure approval process	MB	1/8/17	1/10/17	COMPLETED
2. Information we hold						
2.1	Document what personal data (types) we hold. This needs to include where it came from and who it goes to					
	2.1.1	Create Information Asset Register based on PSN Risk Assessments initially	MB	1/8/17	11/10/17	COMPLETED
	2.1.2	Meet with System administrators to complete the IAR	MB	1/2/18	~~1/2/18~~ 9/3/18	COMPLETED
2.2	Establish the condition for processing the data		Services			
	2.2.1	Gather this data through completion of IAR	MB	11/10/17	~~1/2/18~~ ~~9/3/18~~ 29/3/18	COMPLETED
2.3	Establish if any profiling / automated decision making is being done					
	2.3.1	Gather this data through completion of IAR	MB	11/10/17	1/2/18 9/3/18	COMPLETED
2.4	Record of processing activity					
	2.4.1	Update Record of Processing Activity template to reflect IAR	MB	23/4/18	4/5/18	COMPLETED
	2.4.2	Circulate ROPA to services for agreement	MB	8/5/18	25/5/18	Still awaiting some service input
	2.4.3	Collate Service ROPA updates into master document	MB	1/6/18	28/09/18	
3. Privacy information						
3.1	Review all current privacy notices and update as required					
	3.1.1	Identify all current privacy notices	MB	1/9/17	~~1/11/17~~ 9/3/18	COMPLETED
	3.1.2	Meet with services to discuss where specific privacy notices are required	MB	12/3/18	~~1/2/18~~ 29/3/18	COMPLETED

TASK			LEAD	START DATE	END DATE	UPDATE
	3.1.3	Update / create privacy notices with input from services	Services	3/4/18	~~3/4/18~~ 1/5/18	COMPLETED
3.2	Embed privacy notice signposting into everyday interactions					
	3.2.1	Publish Privacy notice	Comms	1/5/18	11/5/18	COMPLETED
	3.2.2	Update corporate templates to include privacy notice link	Comms	1/5/18	11/5/18	COMPLETED
	3.2.3	Get contact centre recorded message updated to include link to privacy notice	ALC / KB	1/5/18	11/5/18	COMPLETED
	3.2.4	Get PN link included in email 'watermark' on all external emails	ICS	1/5/18	11/5/18	COMPLETED
	3.2.5	Circulate wording for officers answering phones to ensure PN is signposted	MB	1/5/18	11/5/18	COMPLETED
	3.2.6	Update customer service advisors with information they need to be explaining to customers in regards to privacy notices	MB / ALC/ KB	1/5/18	11/5/18	COMPLETED
4. Individual's rights						
4.1	Create procedures around individual's rights					
	4.1.1	Right to be informed	MB	1/1/18	~~1/4/18~~ 23/02/18	COMPLETED
	4.1.2	Right of access	MB	12/3/18	~~1/1/18~~ 19/4/18	COMPLETED
	4.1.3	Right to rectification	MB	12/3/18	19/4/18	COMPLETED
	4.1.4	Right to erasure	MB	12/3/18	19/4/18	
	4.1.5	Right to restrict processing	MB	12/3/18	19/4/18	
	4.1.6	Right to data Portability	MB	12/3/18	19/4/18	
	4.1.7	Right to Object	MB	12/3/18	19/4/18	
	4.1.8	Automated decision-making	MB	12/3/18	19/4/18	

TASK			LEAD	START DATE	END DATE	UPDATE
5. Consent						
5.1	Review how we seek and manage consent for processing					
	5.1.1	Through completion of IAR, create a list of the services we provide relying on consent	MB	1/10/17	~~1/2/18~~ ~~9/3/18~~ 29/3/18	COMPLETED
	5.1.2	Work with services to ensure consent is informed and specific	MB	12/3/18	29/3/18	COMPLETED
5.2	Ensure consent is being recorded					
	5.2.1	Work with services to ensure consent recording process is in place	MB	12/3/18	30/4/18	COMPLETED
6. Children						
6.1	Do we provide Children with services directly based on their consent?					
	6.1.1	Establish (through IAR) whether we require children to provide consent for services – holiday activities?	MB	1/10/17	~~31/1/18~~ 9/3/18	COMPLETED
7. Data Breaches						
7.1	Data Breach Procedure					
	7.1.1	Review breach procedures and publish	MB	1/8/17	1/12/17	COMPLETED
	7.1.2	Communicate to all staff their responsibilities and highlight possible consequences of not doing this	MB	1/1/18	1/4/18	COMPLETED
7.2	Data Breach reporting to ICO					
	7.2.1	Establish when we will need to report breaches to the ICO	MB	1/8/17	29/3/18	COMPLETED
	7.2.2	Keep logs of all breaches and reasons for when these are not reported to the ICO	MB	1/1/18	1/4/18	COMPLETED

TASK			LEAD	START DATE	END DATE	UPDATE
8. Data Protection by Design & Privacy Impact Assessments						
8.1	Review what processes may need PIA		Services			
	8.1.1	Through completion of IAR identify higher risk or high volume processing processes	MB	1/10/17	~~1/2/18~~ 29/3/18	COMPLETED
	8.1.2	Complete PIA for the processes identified in 8.1.1	Services	12/3/18	30/4/18	COMPLETED
	8.1.3	Establish if any PIA needs sign off from ICO – i.e. remains high risk despite mitigation	MB	12/3/18	30/4/18	COMPLETED
8.2	Projects and Procurement					
	8.2.1	Establish procedure to ensure projects and new procurement exercises involve consideration of Data Protection in the initial stages	MB	1/11/17	12/3/18	COMPLETED
	8.2.2	Establish procedure to ensure projects and new procurement exercises either complete a PIA or records why one is not required.	MB	1/11/18	12/3/18	COMPLETED
	8.2.3	Define when PIA's need to be referred to ICO	MB	1/11/17	29/318	COMPLETED
8.3	Establish Roles under GDPR					
	8.3.1	Ensure duties for the Data Protection Officer as set out in the GDPR are set out in Job Description	SJ	1/9/18	31/12/17	COMPLETED
8.4	Records					
	8.4.1	Establish what records are required	MB	1/9/17	31/12/17	COMPLETED
	8.4.2	Ensure records are created and procedures are in place for routinely recording the information required	MB	1/1/18	1/3/18	COMPLETED

TASK			LEAD	START DATE	END DATE	UPDATE
9. Contracts						
9.1	Contracts					
	9.1.1	Identify Contracts which involve contractors processing personal data	MB / DH	1/12/17	23/2/18	COMPLETED
	9.1.2	Notify contractors of changes	MB / DH	5/3/18	16/3/18	COMPLETED
	9.1.3	Update contract clauses	AW	19/3/18	18/5/18	Legal taking forward