Cheltenham Borough Council
Audit Committee – 18 April 2018
Data Protection

Accountable member	**Councillor Roger Whyborn**
Accountable officer	**Director of Resources and Corporate Projects, Mark Sheldon**
Ward(s) affected	**None Directly**
Key/Significant Decision	**No**
Executive summary	From 25 May 2018, the existing Data Protection Act 1998 will be replaced by new legislation in the form of the EU General Data Protection Regulation (GDPR),a new Data Protection Act and related legislation. This report sets out the main features of the legislation and its likely impact, and details the current approach to ensuring compliance. The Council currently has a Data Protection Policy which has been rewritten to reflect the new legislation. This new Data protection Policy (appendix 2) applies to all users who handle information and personal data held by Cheltenham Borough Council, including personal data of our service users. This Policy applies to all employees, Members and processors of personal data held by the Council.
Recommendations	**That Audit Committee consider and comment upon the new Data Protection Policy and recommend to Cabinet that it is approved for use** **That Audit Committee recommend to Cabinet that authority be delegated to the Director of Resources and Corporate Projects to vary the existing s101 Shared Service arrangement between the Council, Gloucester City Council and One Legal (Tewkesbury Borough Council) to:** • Include undertaking the statutory function of the DPO under the Data Protection legislation and • Designate the council's Borough Solicitor as the DPO for the council

Financial implications	Members approved new funding of £17,000 for this council's share of the cost of a new Data Protection Officer, to be provided by One Legal, as part of the Council 2018/19 budget setting meeting on 19th February 2018, as detailed in section 3 of this report. Gloucester City Council and Tewkesbury District Council also have provision for their share of this new cost within their Council budget. **Contact officer: Sarah Didcot** **Tel; 01242 264125** **Email; Sarah Didcot @cheltenham.gov.uk,**
Legal implications	The Data Protection Policy has been updated to reflect the new Data Protection legislation due to come into effect on 25th May 2018. The Data Protection Officer is a statutory role whose responsibilities are set out in the proposed legislation. The proposal is to extend the current s101 shared service arrangement with One Legal to undertake the function. **Contact Officer Shirin Wotherspoon, OneLegal** **Email; Shirin.wotherspoon@tewkesbury.gov.uk** **Tel; 01684 295010**
HR implications (including learning and organisational development)	As stated the existing Data Protection Act 1998 will be replaced by new legislation in the form of the EU General Data Protection Regulation (GDPR), and a new Data Protection Act. The Council is aware of its duty to ensure that the roles, responsibilities and knowledge of the new legislation are cascaded to all employees. Training has been provided by colleagues from Publica and One Legal. **Contact officer: Julie McCarthy, HR Manager, Publica Group Ltd.** **Tel; 01242 264355** **Email; julie.mccarthy@cheltenham.gov.uk,**
Key risks	**If the Council fails to have a robust Data protection process in place or to provide the necessary resources then it will fail to comply with legation which could lead to a data breech, substantial fines and reputational damage.**
Corporate and community plan Implications	None
Environmental and climate change implications	None

1. Background

1.1 Cheltenham Borough Council (CBC) has an obligation to comply with the six Data Protection principles when processing personal data. These principles require that personal data:

- Shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Shall be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.
- Shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
- Shall not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed. Personal data may be stored for longer periods provided it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This is subject to the implementation of appropriate data security measures designed to safeguard the rights and freedoms of data subjects.
- Shall be processed in a manner that ensures its appropriate security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

1.2 CBC will ensure that it is able to demonstrate compliance with all of the above six principles by:

- Following best practice in all personal data processing;
- adhering to the relevant processing conditions for the fair and lawful processing of personal data and special categories of personal data (set out on page 4);
- telling people why we are processing their personal data and who we will share their personal data with, through our clear and effective privacy notices;
- ensuring that if relying on consent from the data subject, it is freely given, specific, informed and unambiguous;
- implementing "privacy by default" measures to ensure that, by default, we only process the personal data necessary for each specific business purpose.

2. The need for a new Data Protection Policy

2.1 From 25 May 2018, the existing Data Protection Act 1998 will be replaced by new legislation in the form of the EU General Data Protection Regulation (GDPR), and a new Data Protection Act. This report sets out the main features of the legislation and its likely impact, and details the current approach to ensuring compliance.

2.2 The Council currently has a Data Protection Policy which has been rewritten to reflect the new legislation.

2.3 This new Data Protection Policy (appendix 2) applies to all users who handle information and personal data held by Cheltenham Borough Council, including personal data of our service users.

2.4 This Policy applies to all employees, Members and processors of personal data held by the Council.

2.5 CBC therefore needs a policy (see recommendation 1) to provide guidance to ensure that the Council is compliant with the legislation and that all of its Data is collected, managed, shared stored and deleted correctly to prevent breaches of the legislation. This policy covers the following key areas:

- Policy Objectives
- Introduction to Data Protection Legislation
- Accountability and Demonstrating Compliance
- Organisational Security
- Handling Personal Data
- Sharing Personal Data and Processing of Personal Data by Third Parties
- Specific Uses
- Monitoring and Review

2.6 The legislation and best practice describes a number of Key roles and responsibilities these are described in the policy.

- SENIOR INFORMATION RISK OWNER (SIRO) - to ensure information assets and risks with the Council are managed as a business, actively work with the DPO and other experts within or outside the Council to determine the most effective and proportionate information control measure. The SIRO is responsible for building an informed culture within the Council to promote the best practice for the use and protection of Information assets.
- SINGLE POINT OF CONTACT FOR CONTROLLER (SPoC) - to act as single point of contact for customers, staff and the Data Protection Officer in relation to Personal Data. Support the SIRO in ensuring the Council can demonstrate compliance with current Data Protection Legislation.
- DATA PROTECTION OFFICER (DPO) - to undertake the statutory role by monitoring compliance and by providing advice and assistance to the SIRO. The DPO may report directly to the Council's Executive Board and shall provide training on policies relating to data protection. INFORMATION ASSET OWNERS - Service managers have been nominated as Information Asset Owners for the information held within their service areas and are responsible for ensuring that their services area can demonstrate compliance with current Data Protection Legislation.
- STAFF - all staff are responsible for ensuring that the Personal Data they handle is processed in accordance with this Policy and current Data Protection Legislation.
- MEMBERS - all members are responsible for ensuring that the Personal Data they handle is processed in accordance with this Policy and current Data Protection Legislation.

2.7 A summary of the key roles of the Data Controller, the Data Protection Officer and the Information Controller is set out in appendix 3.

3. Appointment of Data Protection Officer

3.1 The new legislation also states that the council is required under s67 of the Data Protection Bill and the General Data Protection Regulations 2016 (the Data Protection legislation) to designate a data protection officer (DPO). The Bill provides that the data controller (the council), when designating a DPO must have regard to the professional qualities of the proposed officer, in particular, '..expert knowledge of data protection law and practice' and , ' the ability of the proposed officer to perform the tasks mentioned in s69'.

3.2 S69 of the Bill sets out the tasks of the DPO as follows:

- Informing and advising the controller, any processor and employee of their obligations under legislation
- Advising on data protection impact assessments and monitoring compliance
- Co-operating with the ICO
- Acting as the contact point for the ICO on processing issues
- Monitoring compliance with policies
- Monitoring compliance generally.

3.3 The Bill permits the same DPO to be designated by several controllers.

3.4 On 1st April 2015 the council, Tewkesbury Borough Council and Gloucester City Council entered into a shared service arrangement under s101 of the Local Government Act 1972 and Part 1A Chapter 2 Section 9EB of the Local Government Act 2000 (and related legislation) (the 's101 Shared Service arrangement'). The functions delegated to One Legal (Tewkesbury Borough Council as host authority) already include advice on Data Protection matters and so undertaking the statutory functions of the DPO and designating the Borough Solicitor as the council's DPO would be effected by a simple Deed of Variation to the s101 Shared Service agreement.

3.5 It is proposed, therefore, to delegate authority to the Director of Resources and Corporate Projects to vary the existing s101 Shared Service arrangement with One Legal to:

- Include undertaking the statutory function of the DPO under the Data Protection legislation and
- Designate the council's Borough Solicitor as the DPO for the council.

3.6 Gloucester City Council and Tewkesbury Borough Council have also agreed to the appointment of One Legal to undertake the DPO role. See recommendation 2

4. Alternative options considered

5. Consultation and feedback

5.1

6. Performance management –monitoring and review

6.1

Report author	**Contact officer: Bryan Parsons Corporate Governance Risk and Compliance officer** **Email bryan.parsons@cheltenham.gov.uk,** **Tel;01242 264189**
Appendices	1. Risk Assessment 2. Data Protection Policy 3. Data protection Roles and responsibilities
Background information	1.

Risk Assessment

Appendix 1

The risk				Original risk score (impact x likelihood)			Managing risk				
Risk ref.	Risk description	Risk Owner	Date raised	Impact 1-5	Likeli-hood 1-6	Score	Control	Action	Deadline	Responsible officer	Transferred to risk register
	If the Council fails to agree a comprehensive Data Protection Policy and train its Data users and processors on the requirements of the law then there could be an increased risk of a data breech and substantial fines	Director of Resources and Corporate Projects (SIRO)	16 April 2018	4	3	12	reduce	Draft and agree a Data Protection Policy that will guide data users and processors	May 2018	Director of Resources and Corporate Projects (SIRO)	
	If CBC as a Data Controller fails to take effective action to comply with the GDPR or to act on the recommendations set out in ICO Codes then it could suffer substantial financial and reputational damage.	Director of Resources and Corporate Projects (SIRO	20/06/2017	5	2	10	Reduce	Initiate and deliver a project based on a project Plan with clear objectives, sufficient resources and clear roles and responsibilities.	May 2018	Project manager	
	If the human and / or financial resources required to deliver the project are not identified	Director of Resources and Corporate Projects	20/06/2017	3	3	9	Reduce	"Review initial assessment of resource requirements as part of service	May 2018	SIRO	

	adequately and put in place there may be a failure to deliver GDPR compliance.	(SIRO)						compliance planning.			
	Monitor resource demands and impacts on champions and services and address resourcing implications in the 2018/19 budget"	Director of Resources and Corporate Projects (SIRO)						Monitored by Project team	May 2018	Project Manager	
	If CBC fails to embed ongoing training and compliance to Data Protection legislation within its systems it is more likely to be open to breaches of the legislation leading to possible fines and/or reputational damage	Director of Resources and Corporate Projects (SIRO)	20/06/2017	5	2	10	Reduce	"Successful delivery of the project.	On-going	SIRO	
	Continued ownership of data protection requirements at corporate and service levels following project completion."	Director of Resources and Corporate Projects (SIRO)						Review of all roles involved in the management of Data Protection	Ongoing	SIRO	
	If the organisation is not prepared for the GDPR which	Director of Resources and	16/11/2017	5	2	10	Reduce	Successful delivery of the project.	May 2018	SIRO	

	comes into effect in May 2018, then this may lead to breach of the regulations and consequently fines which may impact on the organisation's financial resources and reputation.	Corporate Projects (SIRO)									

Explanatory notes

Impact – an assessment of the impact if the risk occurs on a scale of 1-5 (1 being least impact and 5 being major or critical)

Likelihood – how likely is it that the risk will occur on a scale of 1-6

(1 being almost impossible, 2 is very low, 3 is low, 4 significant, 5 high and 6 a very high probability)

Control - Either: Reduce / Accept / Transfer to 3rd party / Close