BRIDGEND COUNTY BOROUGH COUNCIL

REPORT TO CABINET

24 APRIL 2018

REPORT OF THE CORPORATE DIRECTOR – OPERATIONAL AND PARTNERSHIP SERVICES

GENERAL DATA PROTECTION REGULATION AND DATA PROTECTION BILL

1. Purpose of Report

1.1 The purpose of the report is to inform Cabinet of the provisions under the General Data Protection Regulation (GDPR) which is due to be enforced on 25th May 2018 and the Data Protection Bill which was announced in the Queen's speech in June 2017.

1.2 To seek approval of the updated Data Protection Policy and note the updated Code of Practice for Data Breaches.

2. Connection to Corporate Improvement Plan / Other Corporate Priority

2.1 There is no direct link to the Corporate Improvement Plan / Other Corporate Priority.

3. Background

3.1 The European Union's GDPR will require all data controllers and processors that handle the personal information of EU residents to implement appropriate and technical and organisational measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. The GDPR introduces stricter requirements than under the current Data Protection Act 1998.

3.2 The Data Protection Bill updates data protection laws in the UK, supplementing the GDPR as well as extending data protection laws to areas which are not covered by the GDPR. It is intended to provide a comprehensive package to protect personal data. The Bill now sits in the House of Commons and the plan is for it to have completed its parliamentary passage and be ready to take effect in May when the EU laws take effect.

4. Current situation / proposal

4.1 The GDPR's provisions and the obligations which they bring are extensive, but the following stand out as materially new, or varied, concepts:

4.2 <u>Consent</u>
The conditions for obtaining consent have become stricter. The data subject must have the right to withdraw consent at any time; and there is a presumption that consent will not be valid unless separate consents are obtained for different processing activities and there is a presumption that forced, or 'omnibus' consent mechanisms will not be valid.

4.3 Children

Under GDPR children are able to give their lawful consent to the processing of their personal data, in connection with the provision of information services, when they are at least 16 years old. However, the GDPR allows for Member States to lower the age, but no younger than 13. The Bill confirms that in the UK children from the age of 13 can give consent for the processing of their personal data in relation to information services. Those under the age of 13 will require the consent of a parent/guardian. The Bill also clarifies that the reference to "information services" does not include preventative or counselling services.

4.4 Transparency

Data Controllers (a person who determines the purposes for which and the manner in which personal data are or are to be processed) must continue to provide transparent information to data subjects at the time their personal data is obtained. Existing forms of fair processing notices will have to be re-examined as the requirements in the GDPR are much more detailed. The information to be provided is more comprehensive and must inform the data subject of certain of their rights and the period for which the data will be stored. The Authority will need to consider its forms of fair processing notices with these new obligations in mind and check that the information is being provided in a clear and easily accessible format.

4.5 Enhanced rights for individuals

The GDPR enshrines a wide range of existing and new rights for individuals in respect of their personal data. These include the right to be forgotten, right to restrict processing, the right to request the porting of one's personal data to a new organisation, the right to object to certain processing activities and also to decisions taken by automated processes.

4.6 Data Protection Officer

The GDPR lays out the requirements for appointing a Data Protection Officer (DPO) as well as their specification, role, duties and relationships with other entities (such as data subjects, controllers and processors). The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices. The DPO is responsible for ensuring that the controller, processor and employees who process personal data understand their obligations, and for providing advice on meeting those obligations. While this obligation explicitly applies to GDPR, it would make sense that the DPO should also be responsible for providing advice for any other data protection laws that are applicable to the Authority.

4.6.1 The DPO's second task is to monitor compliance, including the assignment of responsibilities, awareness-raising and training staff involved in processing operations, and the related audits.

4.6.2 The Information Officer has been appointed as the DPO for the Authority.

4.7 Data Breach Notification

Data controllers must notify data breaches to the Information Commissioner's Office (ICO) where there is likely to be a high risk to the rights and freedoms of natural persons. This must be done without undue delay and within 72 hours of awareness. A reasoned justification must be provided if this timeframe is not met. In some cases, the data controller must also notify the data subject affected without

undue delay. This is burdensome on data controllers however the ICO already expects to be informed about all "serious" breaches. The Authority already has internal procedures in place for handling data breaches and the Code of Practice for Data Breaches (**Appendix 1**) has been updated accordingly.

4.8 Controller and Processor

Data controllers must implement appropriate measures to ensure that the processing of personal data complies with the legislation. A controller must be able to evidence these measures to others, including the ICO. GDPR imposes stringent new requirements for the appointment of processors by controllers including prescribing various matters which must be stipulated in a contract or other legal act.

4.9 Data Protection Impact Assessments (DPIA)

The DPIA is one of the specific processes mandated by the GDPR and will be used to identify specific risks to personal data as a result of processing activities. The process will help the Authority identify and minimise privacy risks and will usually be conducted ahead of implementing new processes, projects or policies. The aim will be to seek out potential problems so that they can be mitigated ahead of time, thereby reducing the likelihood of occurrence and the associated costs.

4.10 Schools

To date, the Authority has provided two training sessions and several monthly updates to Headteacher colleagues in respect of GDPR. A two day workshop event will also take place in May designed to support senior leaders at schools and school governors. While schools are their own data controllers (ie not the local authority), going forward, the Authority will continue to support schools in respect of data protection regulation compliance.

4.11 Next steps

In readiness for GDPR an Implementation Group has been established with appropriate representation from each Directorate.

4.11.1 The Data Retention Policy was approved by Cabinet in January 2018 and stipulates data retention periods for each business area. There is a requirement under current data protection law to not keep information for longer than is necessary and this will continue to apply under GDPR.

4.11.2 A new Data Protection E-Learning Module has been launched which will be mandatory for all staff who process personal data and all Elected Members.

4.11.3 The Data Protection Policy (**Appendix 2**) and Code of Practice for Data Breaches have been updated to ensure they remain fit for purpose.

4.11.4 The relevant pages of the intranet and internet will be updated accordingly.

5. Effect upon Policy Framework& Procedure Rules

5.1 The Data Protection Policy will be amended accordingly.

6. Equality Impact Assessment

6.1 There are no equality implications arising from this report.

7. Financial Implications

7.1 CMB have approved the purchase of redaction software for the Authority to assist with data subject access requests at an estimated cost of £7467 (for three years and three licences) and also the appointment of an Apprentice to support the Information Team and the Social Services and Wellbeing Directorate (where possible to do so). The Apprentice will cost around £40,000 with on-costs for the two years. These costs will be met from a specific earmarked reserve.

8. Recommendation

Cabinet is recommended to:

- Note the report and the enforcement of the GDPR and Data Protection Bill;
- Approve the updated Data Protection Policy attached as **Appendix 2** to take effect from 25th May 2018;
- Note the updated Code of Practice for data breaches attached as **Appendix 1** to take effect from 25th May 2018.

Contact Officer: P A Jolley
Corporate Director – Operational and Partnership Services

Telephone: (01656) 643106
E-mail: Andrew. Jolley@bridgend.gov.uk

Postal Address Civic Offices,
Angel Street,
Bridgend,
CF31 4WB

Background Documents
None