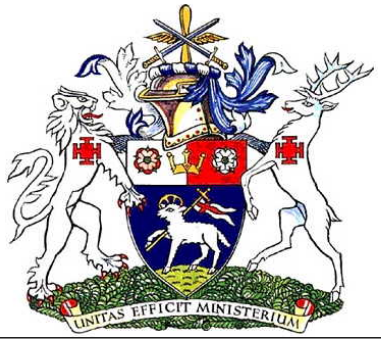	**Policy & Resources Committee** **13 February 2018**
Title	**Council Preparations for the General Data Protection Regulation (GDPR)**
Report of	Councillor Richard Cornelius
Wards	All
Status	Public
Urgent	No
Key	No
Enclosures	None
Officer Contact Details	Victoria Blyth, Information Strategy Manager victoria.blyth@barnet.gov.uk 020 8359 2015 Jenny Obee, Head of IT & Information Management jenny.obee@barnet.gov.uk 020 8359 4859

Summary

The General Data Protection Regulation (GDPR) will apply in the UK from 25 May 2018. The GDPR will replace current Data Protection Act 1998 (DPA) legislation and will bring about a considerable number of changes which organisations will be expected to implement and be able to comply with ahead of this date. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The legislative changes will impact the way the council engages and interacts with its customers and places expectations on it which must be met. This paper provides an overview of the key changes that need to be implemented and highlights key risks or issues that need to be considered as part of the implementation process.

Other legislation, or proposed legislation, such as the Digital Economy Bill, Criminal Information Directive, Network & Information Security Directive, the Lord Chancellor's Code of Practice on the management of records issued under section

46 of the Freedom of Information Act 2000 and the Privacy & Electronic Communications Regulations 2003 will also need to be considered for their interactions with GDPR, as this other legislation also covers the processing of personal data in some respects.

The Information Management Team (IMT) has begun implementing the plan of required actions, however some of the work will need to be undertaken by delivery units, due to their knowledge and expertise in their respective areas, and this will impact on their resourcing.

Officers Recommendations

1. **That the Policy & Resources Committee notes the deadline of 25 May 2018 associated with compliance with the GDPR and the potential regulatory action in the event of non-compliance.**
2. **That the Policy & Resources Committee notes the distinction of the three roles of a councillor, how GDPR applies to each of them, and the split of responsibilities between council and councillor as detailed in section 5.4.5.**
3. **That the Policy & Resources Committee endorses the importance of the planned e-learning detailed in section 5.2.2 and encourages councillors to undertake said e-learning, including any newly elected councillors following the 3 May local elections.**

1. WHY THIS REPORT IS NEEDED

1.1 The General Data Protection Regulation (GDPR) will apply in the UK from 25 May 2018. The GDPR will replace the current Data Protection Act 1998 (DPA) legislation and will bring about a considerable number of changes that organisations are expected to implement and comply with on this date. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR, although the UK is currently working on the Data Protection Bill that is likely to be the way the UK incorporates GDPR requirements into UK law post-Brexit.

1.2 Considerable work is required to ensure compliance with the new legislation. The Information Management Team (IMT) is running a GDPR Implementation Project, however some of the work will need to be undertaken by delivery units, due to their knowledge and expertise in their respective areas. The work both for IMT and delivery units has resourcing implications of employee time and budget. This report provides an overview of the key changes that need to be implemented and highlights key risks or issues that need to be considered as part of the implementation process.

2. REASONS FOR RECOMMENDATIONS

2.1 To ensure that the Policy & Resources Committee notes the deadline associated with compliance with the GDPR on 25 May 2018 and the potential regulatory action in the event of non-compliance.

2.2 To ensure that councillors are aware of the effect GDPR has on their obligations with respect of personal data when acting as ward representative, and are aware of the e-learning for the processing of personal data they undertake on

behalf of the council, especially given that the e-learning will be rolled out during the busy period of April-May 2018.

3. ALTERNATIVE OPTIONS CONSIDERED AND NOT RECOMMENDED

3.1 The council cannot choose to not comply with legislation and therefore has no alternative but to implement appropriate measures to ensure compliance with GDPR on 25 May 2018 and ongoing.

4. POST DECISION IMPLEMENTATION

4.1 The GDPR Implementation Project will continue its work to ensure compliance across the council.

4.2 Employees and councillors will be provided with access to e-learning once the package is procured and implemented.

4.3 Amendments to the council's constitution will be proposed, in line with procedures for constitutional changes.

4.4 Officers propose bringing a further report to committee on implementation and outstanding risks following the introduction of GDPR on 25 May 2018.

5. IMPLICATIONS OF DECISION

5.1 Corporate Priorities and Performance

5.1.1 Most of the services the council delivers and the work it undertakes involves the processing of personal data in some form. The GDPR therefore affects most of the council's work and will bring about a considerable number of changes which the council must implement to be able to comply with the new law. GDPR impacts the way the council engages and interacts with its customers, contractors, partners and staff.

5.1.2 The vision and principles of the council's Information Management Strategy 2016-20 are met through compliance with the GDPR. Deliverables of the GDPR Implementation Project will meet aims of the strategy's delivery framework. For example, through a record of processing we establish ownership and management of information, and support for staff through targeted communications and a revised policy suite.

5.1.3 One of the key tenets of the GDPR is accountability. Not just doing the right thing, but proving compliance with documentation, audit trails and a schedule of compliance and training. Ensuring that the council complies with relevant legislation is not only a legal requirement, but a key way to inspire trust and act in an honourable and transparent way. The GDPR Implementation Project is therefore actively contributing to the five corporate priorities of:

- Delivering quality services
- Responsible growth, regeneration and investment

- Building resilience in residents and managing demand
- Transforming local services
- Promoting community engagement, facilitating independence and building community capacity.

5.1.4 The GDPR requires a Record of Processing Activity (ROPA), which is a corporate register of the processing of personal data that the council undertakes (or causes to be undertaken on its behalf). The GDPR specifies the information that must be captured and in the absence of a council information asset register this task may be substantial for some areas of the council. This task will need to be completed by delivery units for all the work they undertake or cause to be undertaken; and by the council's key partners for the work undertaken under the CSG, Re and Cambridge Education contracts.

5.1.5 The GDPR places an emphasis on privacy and requires a greater level of transparency with data subjects. This will have many impacts on the council as appropriate and evidenced consideration must be given to the GDPR tenets of Privacy by Design and Privacy by Default. This will require undertaking effective Data Protection Impact Assessments (DPIAs), similar to current Privacy Impact Assessments (PIAs), for relevant projects and process changes. A review of the council's project management processes and the governance processes for committee reports and delegated powers decision making is needed to ensure the requirements on privacy are embedded in council processes, much like those for equalities.

5.1.6 Principle One in the GDPR is that personal data shall be processed "Lawfully, fairly and in a transparent manner in relation to the data subject." (art5(1)(a)). Further detail of the requirements of this principle of transparency can be found in articles 12, 13 and 14 of the GDPR, which prescribe a much more detailed notice to data subjects on the processing of their data being undertaken. Whilst the council currently has a corporate privacy notice with a short version on all forms, the information will need to be delivered in a layered privacy notice that provides the level of detail appropriate to each type of data processing taking place. Amending the privacy notice will be a considerable amount of work, partly hindered by the lack of formal guidance available at time of writing.

5.1.7 A review of all council forms (paper and electronic) is also required to ensure that suitable privacy notices are in place. This applies also to specialist privacy notices for those with disabilities or sensory impairments, and where verbal privacy notices are issued (such as over the phone).

5.2 **Resources (Finance & Value for Money, Procurement, Staffing, IT, Property, Sustainability)**

5.2.1 The work required to ensure compliance, such as the ROPA, review of forms and consent, review and amendment of council processes, and implementation of training, will require significant officer time across delivery units.

5.2.2 The council has an obligation to ensure that all those processing personal data on its behalf are appropriately trained and understand their responsibilities. An

e-learning package must be procured and implemented with enough time for all council employees (and councillors) to undertake prior to 25 May. Procurement has been agreed in the 2018-19 forward plan but will likely to need to be brought forward to 2017-18. This will be done through procedures in article 10 of the council's constitution if required.

5.2.3 Under the DPA and GDPR data subjects can make a Subject Access Request (SAR). Under GDPR the maximum deadline for response is shortened from 40 calendar days to 30 calendar days, with the option of charging a £10 fee removed. The loss of the charging mechanism may well increase the number of SARs received and have a small impact on income. From 1 January 2018, the council has shortened the SAR deadline in line with GDPR, to identify any risks for non-compliance prior to the new deadline being in force.

5.2.4 Currently the council is obliged to pay a £500 annual notification fee to the ICO as part of registering its processing activities with them. This fee is scrapped under GDPR. However, as that will leave a £17m budget deficit which will need to be covered to support the function of the ICO, the government has added proposals to the Digital Economy Bill for a charging structure. The new model will go live in April 2018 and while the structure has not yet been finalised it is likely to result in a cost of up to £1,000 per annum for local authorities.

5.2.5 Councillors are currently subject to an annual registration fee of £35 which is managed by council officers and paid from a councillor's notional allowance. It is believed that this fee is likely to either rise to approximately £55 or be scrapped completely.

5.2.6 Local authorities will be required to employ a named Data Protection Officer (DPO) either directly or through contract. The DPO must be appropriately trained and have the professional knowledge and skills to undertake the role. The post cannot be held by someone in a role deemed to conflict with the role of DPO, or a role that has any authority to determine the manner in which data is processed by the council. The DPO must work in an independent manner.

5.2.7 The DPO has many duties which must be undertaken and they will require access to appropriate resource, budget and staffing to complete their role and ensure the council's compliance with GDPR. The role of DPO has certain protections from dismissal, similar to the Monitoring Officer, and must have access to senior management to report issues and request resource. Amendments to the council's constitution will be proposed through normal channels to reflect these responsibilities, duties and protections as appropriate.

The council currently has an experienced and qualified data protection practitioner in post and this position will be amended and re-graded in line with HR processes to reflect the new responsibilities of the DPO.

5.2.8 Under GDPR the breach management and reporting requirements are strengthened, with the monetary penalty limits significantly increased to a maximum of €20m or 4% of turnover (whichever is larger). The ICO has confirmed that it expects organisations to be fully compliant by 25 May 2018

and will consider enforcement action of decision notices, enforcement notices and monetary penalties from that date as it deems appropriate. The council self-funds any monetary penalties and the GDPR Implementation Project has made the insurance and finance teams aware of this increased financial risk.

5.3 Social Value

5.3.1 GDPR clarifies and enhances the rights of data subjects and council processes will be amended where required to ensure that the council meets its legal obligations to individuals under GDPR. This will have benefit to individuals, although the legislation is such that many data subjects will never realise or appreciate the levels to which the council meets high standards in handling their personal data.

5.3.2 The increased emphasis on privacy as discussed in 5.1.5 puts the rights of the individual at the forefront of any project or process change and requires that the council considers privacy impacts at the earliest stage in planning and decision making.

5.3.3 Changes to the SAR deadline and charging mechanism makes the process easier to access for individuals, but may have an impact on the number of requests received and therefore the resource required from the council.

5.4 Legal and Constitutional References

5.4.1 Article 7 of the Council Constitution, under responsibility for function sets out the terms of reference of Policy and Resources Committee including to be responsible information technology and for those matters not specifically allocated to any other committee affecting the affairs of the Council.

5.4.2 HBPL will be asked by the project to identify any risks to current council contracts and/or assure the council that standard contract clauses adequately cover GDPR and attendant legislation that affects the processing of personal data as listed in this report's summary.

5.4.3 The duties and responsibilities of the role of DPO as mentioned in 5.2.6 and 5.2.7 will require amendment to the council's constitution.

5.4.4 Amendments required to council processes as mentioned in 5.1.5 may require changes to the council's constitution or constitutional processes.

5.4.5 Mandatory breach reporting for incidents that meet criteria is required under GDPR, within 72 hours of the council becoming aware of the incident. This short deadline will mean that officers must act quickly and expedite the reporting of incidents to the Information Management Team, in line with council policy. Criteria for reporting incidents to the ICO are much tighter under GDPR. However, as the council takes a transparent approach to reporting incidents to the ICO, it is not clear at present whether GDPR will mean an increase in the incidents reported. Further ICO guidance is expected.

5.4.6 In terms of information legislation, elected Members of a local authority are considered to fulfil three roles:

1. They act as a Member of the Council (eg as a member of a committee).
2. They act as a representative for residents of their ward.
3. They may represent a political party, especially at election time.

These three roles have different responsibilities under information legislation. Councillors in their role as Member of the Council are covered by the council's responsibilities under GDPR and it is the council's obligation to ensure that Members understand their responsibilities and have undertaken appropriate training. The council does this partly through the Members' Information Management Policy. When the council rolls out e-learning training in preparation for GDPR it strongly recommends that all Members undertake the training in order to understand their responsibilities and limit the risk to the council of non-compliance with GDPR.

Councillors are solely and individually responsible for their processing of personal data in their role as ward representative and the council has no obligation to undertake work for them or provide training for them for this role. However, the training undertaken for their role as Member of the Council is generally applicable to their work as ward representative. More details of the breakdown of the roles of a councillor can be found in the Members' Information Management Policy on the council's intranet and website.

Political parties, if a councillor is a member, are responsible for the processing of personal data by councillors in their third role.

5.5 Risk Management

5.5.1 A lack of preparation resulting in non-compliance and failure to meet new legislation could result in formal action, including monetary fines, issued to the council and/or contracted partners. The GDPR Implementation Project is in progress to mitigate these risks, although contractors also have their own responsibilities under GDPR.

5.5.2 Under the new legislation, monetary penalties increase considerably from a maximum of £500,000 (under current data protection legislation) to a maximum of €20m or 4% of turnover (whichever is greater). The council self-funds any monetary penalties and the GDPR Implementation Project has made the insurance and finance teams aware of this increased financial risk.

5.5.3 Inadequate resource will result in the council failing to meet its legal obligations; raising concerns over safeguarding and inappropriate processing of personal data. Inadequate resource will have an impact on whether the council can comply with its obligations for accountability, an emphasis on privacy at the start of and throughout projects, and individuals' rights.

5.6 Equalities and Diversity

5.6.1 Whilst the council has an overarching privacy notice, delivery units ensure that the processes for gaining consent and informing customers of what will be

happening with their personal data are appropriate. The council already makes reasonable adjustments for data subjects who have disability, impairment or sensory loss and this will need to continue under GDPR. The project and delivery units will consider children and how to be transparent with them about where and how their data is being processed.

5.7 **Corporate Parenting**

5.7.1 The GDPR specifies that children's consent should be respected, sometimes instead of parental consent. The impact of this will be considered and incorporated into council processes when further guidance is issued by regulatory or advisory bodies.

5.8 **Consultation and Engagement**

5.8.1 The council is responsible for all data processed on its behalf, therefore Re, CSG and Cambridge Education will be included in this project's work, as well as any smaller contractors working on the council's behalf. The GDPR Implementation Project is engaging with all delivery units through their Information Management Governance Groups (IMGGs), and through the Commercial Team with key contractors (Re, CSG, Cambridge Education). Delivery units will be engaging directly with their contractors. Any currently commissioned services returning to sit directly under the council need to be assessed to identify actions needed for GDPR compliance, including entry on the ROPA. This responsibility must lie with the project teams managing any insourcing.

5.8.2 The Barnet Group and HBPL are separate data controllers and will make their own arrangements for GDPR.

5.8.3 Schools are also excluded from the project, as they are their own data controllers. However, where appropriate general guidance will be provided by the council to assist schools.

5.8.4 The council's privacy notice will be considerably amended to meet GDPR requirements and communication of the change will be made to residents through conduits like the council's website and the annual council tax letters issued in March/April.

5.8 **Insight**

5.8.1 GDPR legislates on the nature of 'profiling' activities involving personal data. Our contractor and supplier of the Insight service is reviewing their work in light of GDPR, to identify whether any insight work currently undertake will be affected or need amendment to process or outcomes.

6. BACKGROUND PAPERS

6.1 None**.**