THE GENERAL DATA PROTECTION REGULATION

Cabinet Member(s)	Councillor Ray Puddifoot MBE Councillor Jonathan Bianco
Cabinet Portfolio(s)	Leader of the Council Finance, Property and Business Services
Officer Contact(s)	Raj Alagh - Chief Executive's Office
Papers with report	**Appendix 1** - Data Protection Policy **Appendix 2** - Golden Rules for Protecting Personal and Sensitive Data **Appendix 3** - Information Governance Policy **Appendix 4** - Lawful Basis for Processing of Personal Data Policy **Appendix 5** - Data Protection Individuals' Rights Policy **Appendix 6** - Right of Subject Access Policy **Appendix 7** - Procedure for Undertaking a Data Protection Impact Assessment **Appendix 8** - LBH Generic Data Protection Privacy Notice **Appendix 9** - Record of Processing Activities Form **Appendix 10** - Procedure for Reporting Information Security Breaches, Data Protection Breaches & Card Data Security Incidents **Appendix 11** - ICT Acceptable Usage Policy **Appendix 12** - Document Retention and Destruction Policy

HEADLINES

Summary	This report outlines the new data protection laws which are due to come into force on 25 May 2018. It sets out the steps which the Council has taken to prepare for the new data protection regime and it seeks Cabinet's approval to the new policies and procedures which have been introduced as part of the preparatory work.
Putting our Residents First	This report meets the Council's objectives of our people. Residents expect the Council to take all necessary steps to safeguard and protect their personal information and privacy generally.
Financial Cost	None directly arising from this report.
Relevant Policy Overview Committee	Corporate Services, Commerce and Communities
Relevant Ward(s)	All Wards

RECOMMENDATIONS

That Cabinet:

1. **Notes the contents of the report.**

2. **Approves the Data Protection Policies and Procedures as set out in Appendices 1-12.**

3. **Delegates authority to the Borough Solicitor, in consultation with the Leader of the Council and the Cabinet Member for Finance Property and Business Services, to introduce any new Data Protection Policies and Procedures which are necessary to ensure that the Council is at all times fully compliant with the General Data Protection Regulation and the Data Protection Act 2018.**

4. **Agrees that all Members of the Council should receive training from the Borough Solicitor on the General Data Protection Regulation and the Data Protection Act 2018.**

5. **Requests that the Chairman of the Executive Scrutiny waives the scrutiny call-in period so that any decisions can take immediate effect. This will ensure that the Council's Data Protection Policies and Procedures are in place and published on the Council's Website ahead of the new Data Protection Laws coming into force.**

Reasons for recommendations

The laws on data protection have been overhauled by European and Domestic Legislation and the Council needs to ensure that it is fully compliant with them and to evidence its compliance by having a set of robust policies and procedures in place.

Alternative options considered / risk management

The GDPR and the Data Protection Bill, once enacted, will introduce a new data protection regime and standard and the Council, in its capacity as a data controller, has no option other than to fully comply with the new set of laws.

Policy Overview Committee comments

None at this stage.

SUPPORTING INFORMATION

Background

The General Data Protection Regulation [GDPR]

1. The GDPR is a European Directive which comes into force on 25 May 2018. It creates a new data protection standard that applies to all Member States in the European Union. In very broad terms, the GDPR sets out the respective responsibilities of data controllers, such as the Council, data processors who are responsible for processing personal data on behalf of the Council and data subjects who are individuals whose personal data is being processed.

2. The GDPR defines 'personal data' as any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified directly or indirectly. The GDPR applies to:

- all personal data that is processed automatically;
- any personal data held in a manual form in a relevant filing system;
- any personal data held in an accessible record.

The most common examples of personal data are individuals' names, addresses, dates of birth etc.

3. A number of very significant changes have been introduced by the GDPR which are summarised in the report.

The Data Protection Bill

4. The UK Government has introduced a Data Protection Bill which is intended to give domestic effect to the GDPR. The GDPR provides an overall data protection framework and the Bill, once enacted, will fill in a number of gaps in the framework and provide a much more detailed set of statutory provisions which will take effect in the UK. The new Act will have to be read together with the GDPR on the basis that some provisions within the Act will apply where the GDPR is silent and vice versa.

5. The new Data Protection Act, once in force, will repeal the existing Data Protection Act 1998 which has now been in force for twenty years. Technology has significantly developed in that time and the new data protection regime is intended to provide for the 'new digital age'.

6. The Data Protection Bill has passed through the various Parliamentary stages in the House of Lords and it is currently still being considered by the House of Commons. As recently as 9 May 2018, the Bill received its Third Reading and it has also completed the Report Stage. The only stage left to be completed is the consideration of amendments to the Bill and it will then be ready to receive Royal Assent which is anticipated to be 25 May 2018. It is not yet known what the final form of the Act will be.

Summary of changes introduced by the GDPR.

7. In contrast, the GDPR has been finalised and it has made a number of very fundamental changes to data protection laws which are summarised as follows.

I. The Requirement on the Council to appoint a Statutory Data Protection Officer [DPO]

8. The DPO is responsible for ensuring that the Council fully complies with the GDPR and the new Data Protection Act [DPA]. He is required to have a direct reporting line to the Chief Executive and the Borough Solicitor and Monitoring Officer has assumed this role for the Council. His statutory duties include:

- informing and advising the Council and its Members and officers who process individuals' personal data;
- monitoring compliance with the GDPR and DPA and the Council's data protection policies and procedures;
- providing advice in relation to Data Protection Impact Assessments and monitoring their performance;
- acting as the Council's contact point for the Information Commissioner's Office [ICO] on all matters relating to data protection;
- cooperating fully at all times with the ICO.

9. The DPO has drafted a Data Protection Policy, a set of Golden Rules for Protecting Personal and Sensitive Data and an Information Governance Policy which are respectively attached as Appendices 1,2 and 3 to the report.

II. The Rules on obtaining Consent from Individuals have changed

10. If the Council obtains consent from an individual to process their personal data, this constitutes a lawful basis for the processing of the data. The GDPR sets a high standard for consent and it stipulates that an indication of consent must be unambiguous and involve a clear affirmative action. Consent can no longer be inferred. The Council is required to keep clear written records to demonstrate that consent has been given by an individual.

11. The GDPR also gives an individual a specific right to withdraw consent. The Council is required to inform people of their right to withdraw and to offer them easy ways to withdraw their consent at any time.

12. A new Policy has been devised on the Lawful Basis for Processing of Personal Data, which incorporates the new rules on consent, and it is attached as Appendix 4 to the report.

III. Individual Rights

13. A key feature of the GDPR is that data controllers such as the Council are required to process individuals' personal data in a transparent manner and therefore it has provided for the following rights for individuals:

- the right to be informed about the collection and use of their personal data;
- the right to request that their inaccurate personal data is rectified;
- the right to request that their personal data is erased. This is also known as 'the right to be forgotten';
- the right to request that the processing of their personal data is restricted;
- the right to data portability which allows individuals to obtain and reuse their personal data across different Council services;
- the right to object to the processing of their personal data;
- the right not to be subject to automated decision making including profiling.

14. The DPO has devised a new Data Protection Individuals' Rights Policy which is attached as Appendix 5 to the report.

15. The GDPR has also introduced a new right of access for individuals to their personal data which the Council is holding. Under the Data Protection Act 1998, individuals could submit a subject access request to the Council on payment of a £10 fee. The Council had a period of 40 days in which to respond to the request. The GDPR has shortened this timescale to one calendar month and the requirement to pay a fee has been dispensed with. This will place an additional burden on the Council as it is anticipated that there will be a significant increase in the number of subject access requests made to it. A new Right of Subject Access Policy has been drafted which is attached as Appendix 6 to the report.

IV. Data Protection Impact Assessments

16. Both the GDPR and the DPA require that carrying out a Data Protection Impact Assessment [DPIA] is mandatory in certain circumstances. A DPIA is a process to help identify and minimise the data protection risks of a particular Council project when the processing of personal data is likely to result in a high risk to individuals' interests. The GDPR requires the Council to carry out a DPIA if it plans to:

- systematically monitor a public place on a large scale by for example, installing CCTV cameras;
- process sensitive personal data or criminal offence data on a large scale;
- process personal data that might endanger an individual's health or safety in the event of a security breach;
- process personal data that concerns vulnerable adults or children.

17. A Procedure for undertaking a DPIA has been drafted which includes a template for the use of officers and it is attached as Appendix 7 to the report. It should be noted that the Council is required to consult with data subjects or their representatives in relation to the intended processing as part of the DPA process.

V. Data Protection Privacy Notices

18. The Council is required by law to publish a Privacy Notice. Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. Articles 13 and 14 of the GDPR specifically prescribe the type of information which should be included in a Privacy Notice. This includes the purposes of the processing for which the personal data are intended, the legal basis for the processing, the period for which the personal data will be stored, an individual's right to request from the Council, access to and rectification or erasure of their personal data, and also the right to object to the processing of their data.

19. The DPO has drafted a Generic Data Protection Privacy Notice for the Council which is attached as Appendix 8 to the report. He has advised that each service within the Council will also need to prepare their own Privacy Notices in readiness for the commencement date of the GDPR. These Notices are in the process of being drafted at the time of writing the report.

VI. Record of Processing Activities

20. Article 30 of the GDPR requires the Council to maintain a record of processing activities under its responsibility. The types of matters which should be included in the record can best be demonstrated by the Record of Processing Activities Form which is attached as Appendix 9 to the report. This form will need to completed for each service area and the teams within them across the whole of the Council from 25 May 2018.

VII. Reporting Data Protection Breaches

21. Two very significant changes have been introduced by the GDPR in relation to data protection breaches. The first imposes an obligation on the Council to notify the ICO of a breach within 72 hours of it occurring. Failure to do so may result in a fine of up to 10 million Euros [£8.8m] being imposed on the Council.

22. The second change is that the ICO has the power to impose a fine up to 20 million Euros [£17.6m] if a data protection breach occurs within the Council. A procedure for reporting information security breaches, data protection breaches and card data security incidents has been drafted by the DPO and is attached as Appendix 10 to the report.

ICT Acceptable Usage Policy

23. As part of the Council's preparations for the GDPR and the DPA, it has taken the opportunity to review its ICT Acceptable Usage Policy and it has been updated accordingly in order to take into account the new statutory requirements. A copy of the Policy is attached as Appendix 11 to the report.

Document Retention and Destruction Policy

24. The Council has a statutory responsibility to retain and destroy all of its records in accordance with the requirements of the GDPR, the DPA and indeed other relevant

legislation. ‘Data minimisation’ lies at the heart of the new data protection regime and both the GDPR and the DPA stipulate that personal data shall not be kept longer by a data controller than is necessary for its purpose. Therefore, a Document Retention and Destruction Policy has been devised with the objective of providing guidance in this respect. A copy of this Policy is attached as Appendix 12 to the report.

Data Mapping

25. The DPO has requested that a data mapping exercise is conducted throughout the Council. The purpose of this is to try to capture, by categories, details of as much of the personal data that the Council handles and processes as possible. This will serve a number of purposes. Firstly, it will assist the Council in making records of its processing activities by avoiding unnecessary duplication. If data has already been recorded by category, then there is no need to repeat this process. Secondly, the data mapping exercise will help to develop schedules which will be attached to the Document and Destruction Policy. The information which has been obtained will assist the Council in determining how long it is required to keep certain records and documents. Finally, the data mapping exercise can, when completed, be translated into an Information Asset Register which can be placed on the Council's Website. This register will provide a comprehensive overview of the personal data which the Council holds which will further evidence the Council's overall compliance with the new data protection regime.

26. Although a great deal of work has already been done, the data mapping exercise is still work in progress and therefore it does not at this stage form part of the report.

Practical Steps

27. The Council is taking a number of steps to ensure that documents and files within the Council are properly stored and that there is provision for sensitive and confidential information to be kept in cabinets, pedestals etc. which are lockable. This will assist officers in ensuring that they comply with the Golden Rules for Protecting Personal and Sensitive Data, thereby avoiding the potential for data protection breaches.

Training and Awareness

28. A series of nine separate one hour training sessions on the GDPR and the DPA were held for Council officers in March 2018. The Council has also introduced an e-learning module on the GDPR which is mandatory for all officers in the Council to complete.

29. The DPO has also attended a number of staff and management meetings across the Council for the purpose of raising awareness of the requirements of the new data protection regime.

Members

30. Members are data controllers in their own right and now that a new Council is in place, it is imperative that they also receive training on how to meet their obligations under the GDPR and the DPA. Given that the new laws are shortly due to come into

force, this training should ideally take place as soon as possible. The DPO will also assist Members in preparing any documents which are required to demonstrate compliance with the GDPR and the DPA.

Financial Implications

There are no direct financial implications arising from the report. However, as set out in the report there are two changes being introduced as part of GDPR, which will potentially have significant financial implications. Failure to report a breach to the ICO will carry a fine of up to £10 million Euros (£8.8m) and data breach fines will be up to 20 million Euros (£17.6m). These are significantly higher than fines under the current regime.

RESIDENT BENEFIT & CONSULTATION

The benefit or impact upon Hillingdon residents, service users and communities.

Compliance with the GDPR and the DPA by the Council will assure its residents that their personal data is being handled and processed in a responsible and secure manner and that this will in turn minimise the risks of any data protection breaches occurring.

CORPORATE CONSIDERATIONS

Corporate Finance

Corporate Finance has reviewed the report and concur with the financial implications set out above noting the significant increase in potential fines that can be imposed under the new GDPR regime.

Legal

The Borough Solicitor is the author of the report and all necessary legal implications are therefore contained in the body of the report.

BACKGROUND PAPERS

NIL