Inverclyde council

AGENDA ITEM NO: 16

Report To:	**Policy and Resources Committee**	**Date:**	**22 May 2018**
Report By:	**Head of Legal & Property Services**	**Report No:**	**LP/051/18**
Contact Officer:	**Gerard Malone**	**Contact No:**	**01475 712710**
Subject:	**General Data Protection Regulation**		

1.0 PURPOSE

1.1 The purpose of this report is to advise the Policy and Resources Committee of the main provisions of the new EU General Data Protection Regulation ("GDPR") and the preparatory work being undertaken by the Council to achieve practical compliance with the GDPR by the implementation date of 25 May 2018.

2.0 SUMMARY

2.1 The GDPR will come into force on 25 May 2018, notwithstanding Brexit. A new Data Protection Bill to ensure the new data protection laws contained in the GDPR continue to apply as national law in the UK following Brexit is currently progressing through Parliament.

2.2 GDPR is the most significant change to data protection law in over 20 years and will mean important changes to the way in which the Council addresses Data Protection compliance. As well as enhancing existing rights and introducing new rights for individuals, the monetary penalties for a data protection breach will increase from a maximum of £500,000 to 20 million Euros, with a maximum fine of up to 10 million Euros for failure to comply with the GDPR. The reputational damage for an organisation which fails to comply with GDPR will also be considerable.

2.3 This report sets out the main changes to data protection laws which will be introduced by GDPR and highlights the work being undertaken by the Council, led by the recently established Information Governance team, to ensure compliance with the GDPR by 25 May 2018.

3.0 RECOMMENDATION

3.1 It is recommended that the Policy and Resources Committee notes the contents of this report, including the main provisions of the GDPR and the preparatory steps being undertaken by the Council to achieve practical compliance with the GDPR by the implementation date of 25 May 2018.

Gerard Malone
Head of Legal & Property Services

4.0 BACKGROUND TO GDPR

4.1 The GDPR was formally adopted on 4 May 2016 and is set to repeal and replace most EU data protection legislation, including the Data Protection Act 1998 (the "DPA") in the UK, with a much more onerous regime. The GDPR will have direct effect without the need for national legislation. It will apply from 25 May 2018.

4.2 Following the UK's departure from the EU, the European Commission will have to decide whether the UK has an adequate level of protection to allow transfers of personal data to and from the European Union. In August 2017, the UK Government released its Statement of Intent setting out proposals for a Data Protection Bill to ensure the new data protection laws contained in the GDPR continue to apply as national law in the UK following Brexit. This Data Protection Bill is currently progressing through Parliament.

4.3 Whilst the DPA provides for a maximum fine of £500,000 for a serious breach by a Data Controller. The GDPR establishes a two tiered system of administrative fines. Infringements relating to, for example, a failure to record or adequately record processing activities are subject to fines of up to 10 million Euros. Infringements involving basic principles attract higher fines of up to 20 million Euros.

4.4 In the UK the Information Commissioner's Office (ICO) regulates the enforcement of the DPA. Under the GDPR, the regulator will be known as the Supervisory Authority and will continue to be the ICO. The ICO's enforcement powers will be strengthened to include powers to issue warnings, reprimands and orders to Data Controllers, the power to impose temporary and final bans on processing and to order the rectification or erasure of personal data.

4.5 Remedies available to individuals have also been strengthened under the GDPR to include the right to claim compensation from Data Controllers and Data Processors for damage caused by a breach of the GDPR and to an effective judicial remedy against Data Controllers and Data Processors for non-compliant processing of personal data.

5.0 MAIN PROVISIONS OF THE GDPR

5.1 Part 1 of Appendix 1 of this report highlights the main changes to data protection laws which will be introduced by the GDPR. These changes include greater accountability in the way Data Controllers handle personal data and the need to consider the implications for individuals in advance before carrying out certain processing activities. In addition, the GDPR provides greater transparency to data subjects with regard to knowing what their personal data is being used for and strengthens the rights and control individuals have over their personal data. For the first time, there will be a mandatory legal obligation to report any serious data protection breach to the ICO.

5.2 Part 2 of Appendix 1 of the report sets out the actions needed to ensure GDPR compliance by 25 May 2018. These actions have been incorporated into the Council's GDPR Implementation Plan, which is based on the ICO's guidance "Preparing for the Data Protection Regulation – 12 steps to take now". Appendix 2 is a summary of the Council's GDPR Implementation Plan.

6.0 INFORMATION GOVERNANCE TEAM AND DATA PROTECTION OFFICER

6.1 The Council already has a robust Council wide Information Governance Framework and in order to ensure continued delivery of this framework, including GDPR preparation and ongoing GDPR compliance, a dedicated Corporate Information Governance resource has been established within Legal and Property Services. This resource is under the responsibility of the Legal Services Manager and comprises an Information Governance Solicitor and the Complaints Officer.

6.2 As a result of the implications the GDPR will have for Elected Members in respect of their constituency and Council work, the Information Governance team will provide Elected

Members with support, including training sessions, throughout the GDPR implementation phase and beyond.

6.3 The Information Governance Solicitor has also been appointed to the statutory role of the Data Protection Officer (DPO). The key tasks of the DPO are to inform and advise the Council and its employees about their obligations to comply with the GDPR and other data protection legislation; to monitor compliance with the GDPR and other data protection legislation (which includes managing internal data protection activities); to advise on data protection impact assessments; to train staff and conduct internal audits; to be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc.); and to have due regard to the risk associated with the Council's data processing operations. The GDPR provides that the DPO should have a sufficient degree of autonomy and explicitly provides that an organisation must support its DPO by "providing resources necessary to carry out tasks and to access personal data and processing operations and to maintain his or her expert knowledge".

6.4 The creation of the Corporate Information Governance team has been supported by the allocation of £150,000 of earmarked reserves as part of the 2018/19 budget to fund systems improvement and compliance and a training programme.

7.0 GDPR IMPLEMENTATION PLAN - PROGRESS

7.1 The Information Governance team is leading the Council preparation in the GDPR Implementation Plan, assisted by the GDPR Working Group (which is made up of representatives from each Council service known as GDPR Champions) and the Information Governance Steering Group.

7.2 As stated at Paragraph 5.2 above, the GDPR Implementation Plan contains 12 steps and includes actions in respect of training and awareness raising, auditing and documenting information held by the Council, identifying the legal basis for processing information, thinking about how best to communicate privacy information to the public, considering how consent is sought, obtained and recorded, ensuring that data breach management procedures are adequate, considering the impact of GDPR on new and existing Council contracts, implementing relevant changes to processes and systems to comply with new rights of individuals and the designation of a statutory DPO.

7.3 Implementation of these actions is progressing and the plan is being updated as further guidance becomes available from the ICO and the EU. All data protection policies and procedures are being reviewed and updated as necessary. GDPR training and awareness raising is being incorporated into a GDPR specific e-learning module which will be mandatory for all employees who have access to a computer and process personal data. GDPR briefing sessions are to be held for all employees at team leader level and above. A communications plan has been developed to ensure that all employees are aware of GDPR and any changes which may affect the way they work. This involves the issue of briefing notes, pocket guides and regular updates on ICON (including a dedicated FAQs page). Managing the communication of changes to public will be divided into legacy data (existing data) and new data post 25 May 2018. Consideration will be given to the methods of communication in particular with legacy data to minimise duplication of notification of the changes with the public and selecting the most effective communication channels to optimise the effectiveness of message being received.

7.4 GDPR implementation also has implications for Elected Members as they are individual data controllers in their own right in relation to information processed as part of their constituency work. Training sessions focusing on how GDPR will affect Elected Members were held on 25 and 30 April 2018. The Information Governance Team will continue to provide all necessary support to Elected Members throughout the implementation phase and beyond.

8.0 IMPLICATIONS

Finance

8.1 Financial Implications:

One off Costs

Cost Centre	Budget Heading	Budget Years	Proposed Spend this Report £000	Virement From	Other Comments
Information Governance	Training and Systems	2018/19	150		

Annually Recurring Costs/ (Savings)

Cost Centre	Budget Heading	With Effect from	Annual Net Impact £000	Virement From (If Applicable)	Other Comments
N/A					

Legal

8.2 The Council requires to take steps as identified in this report to comply with the terms of the new EU General Data Protection Regulation by the implementation date of 25 May 2018.

Human Resources

8.3 HR are providing assistance by facilitating the launch of the GDPR specific e-learning module.

Equalities

8.4 There are no direct equalities implications arising from this report.

Repopulation

8.5 There are no direct repopulation implications arising from this report.

9.0 CONSULTATIONS

9.1 The Corporate Management Team has been consulted in the preparation of this report.

10.0 LIST OF BACKGROUND PAPERS

10.1 ICO's guidance "Preparing for the Data Protection Regulation – 12 steps to take now" - https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

GDPR – What is new or different?

PART 1

This section highlights the main changes which will be introduced by the GDPR.

Consent

Consent as a legal basis for processing personal data must be freely given, specific, informed and unambiguous and be given by a statement or by a clear affirmative action. These new provisions will in practice make it more difficult to obtain consent. Any implied consent relied upon for data processing activities will require to be reviewed and adapted as mere acquiescence such as silence or the failure to un-tick a ticked box will not constitute valid consent.

Privacy Notices

Although organisations currently have obligations to provide notice of processing activities to Data Subjects, often through the use of privacy notices, again the GDPR sets a higher standard by adding significant additional information requirements which must be provided. This includes advising Data Subjects of the period for which the data will be stored, the data source, and the legal basis for processing as well as the additional new rights afforded to the Data Subject under the GDPR such as the right to withdraw consent to processing where this is the legal basis for processing. The GDPR provides for exceptions to these requirements in specific circumstances. It is understood that the GDPR is intended to lead to a standardised single privacy notice.

Accountability

Currently, most Data Controllers require to submit an annual processing notification to the ICO. This notification system is abolished by the GDPR. Instead, Data Controllers and Data Processors must keep detailed records of their processing activities and make these available to the ICO on request. Data Controllers must also be able to demonstrate that their processing activities are performed in accordance with the requirements of the GDPR. Data Controllers are expected to comply with any Codes of Conduct published in this respect.

Appointment of Data Protection Officer

Public authorities require to appoint a Data Protection Officer under the GDPR. This person will be the first point of contact for the ICO. This is a governance role, which must report to the highest level of management and be able to take decisions on an independent basis with there being no risk of disciplinary action for so doing. The person appointed must have professional experience and knowledge of data protection laws and be provided with adequate resources to meet the Council's obligations under the GDPR. This person should be appointed in advance to take the Council through this change process, informing the organisation and monitoring compliance with the GDPR.

Data Breach Reporting

For the first time the GDPR imposes a system of mandatory notification to the ICO of any data protection breach which is likely to result in risk to the rights and freedoms of individuals. Any such breach must be notified without undue delay and where feasible, no

later than 72 hours of becoming aware of the breach. Data Subjects may also require to be notified in such circumstances.

Subject Access Requests
Under the GDPR individuals are entitled to receive more information without having to pay a fee unless the request is excessive. The time limit for responding to a subject access request is also reduced.

Data Protection by Design
Data Controllers are required to implement appropriate technical and organisation measures designed to implement data protection principles and to integrate the necessary safeguards into processing to meet the requirements of the GDPR. In addition, measures must be implemented to ensure that only personal data necessary for a specific purpose is processed. This will involve restricting access and storage. Appropriate measures may be identified through the use of privacy impact assessments.

Privacy Impact Assessments
Data Controllers must carry out impact assessments where processing is likely to result in a high risk to the rights and freedoms of individuals. Such assessments must be carried out prior to the processing and must contain prescribed information as a minimum. The ICO should publish a list of the processing which would require an impact assessment. Data protection compliance measures must be built into any new process, for example, the installation of a new IT system.

Data Processors
Data Controllers will be subject to all provisions of the GDPR but for the first time, Data Processors will also be subject to some of the provisions of the new laws contained in the GDPR. Further, in terms of the GDPR, Data Controllers must impose more detailed contractual obligations on Data Processors who process personal data on their behalf to ensure compliance. New obligations include, for example, the Data Processor being subject to confidentiality obligations and being contractually obliged to return or delete personal data at the termination or expiry of the processing contract.

PART 2
SUMMARY OF REQUIRED ACTIONS

Drawing on the main changes set out above, in summary, in order to be ready for the implementation of the GDPR, Council will plan its approach to GDPR compliance by:

1. Analysing what data is collected by the Council, how we use such data and identifying to whom we do or may disclose such data;

2. Creating a record, which must be duly updated where necessary, detailing the outcomes of 1. above as well as confirming the legal basis for any processing which takes place;

3. Identifying where consent is relied upon by Council Services as the legal basis for processing and ensuring the obtaining of such consent meets the new higher standard under the GDPR or alternatively, considering whether the Council can rely on another legal basis for relevant processing activities;

4. Considering and updating existing Council privacy and other notices which advise Data Subjects what the Council does and will do with their data and determining how to communicate this to Data Subjects;

5. Considering and updating existing processes and systems which implement the legal right of Data Subjects to access the personal data the Council holds on them though subject access;

6. Considering how to comply with the privacy by design requirements including when it is possible to anonymise personal data and when a privacy impact assessment is required;

7. Considering the appointment of the Data Protection Officer;

8. Ensuring the Council can identify and has processes in place to ensure compliance with data breach reporting requirements;

9. Considering whether existing Data Processing Agreements require to be updated;

10. Considering the impact of the GDPR on existing Council policies; and

11. Making staff aware of the terms of the GDPR and training staff in all of the above matters to the extent the above impacts on their daily tasks.

APPENDIX 2

Summary GDPR Implementation Plan

Code	Task	Who	Target Date	Status at April 2018
GDPR 1 Accountability and Governance				
1.1	**Mandatory GDPR e-learning course** to be placed on Brightwave. This will be targeted to staff who have email access, and handle personal data. Completion rates will be monitored.	Information Governance Team HR & OD	25/5/18	Green – On Track
1.2	**GDPR Pocket Guide** to be issued to staff to be able to access and refer to as matters arise.	Information Governance Team Corporate Communications	18/5/18	Green – On Track
1.3	**Staff Training** in preparation for legislation coming into force. Training will be available on a regular basis following GDPR implementation.	Information Governance Team	25/5/18	Green - On Track
	Elected members – scheduled dates in diary		25/4/18 30/4/18	Green - Training completed.
	Team Leaders & Managers – Key influencers – scheduled dates in diary		8/5/18 15/5/18	Green - Scheduled – On Track
	Head teacher's – scheduled dates in diary		16/5/18	Green - Scheduled – On Track
	Customer Services– scheduled dates in diary		16/5/18 23/5/18	Green - Scheduled – On track
1.4	**GDPR Guide** to be prepared for Elected Members.	Information Governance Team Corporate Communications	18/05/18	Green – in progress
1.5	**Policies & Procedures -** all relevant polices require updating.	Information Governance Team	25/05/18	Green - Ongoing
1.6	**Service Provision Forms –** changes to internal forms to ensure they are GDPR compliant. Statutory forms will be changed through relevant owners.	Information Governance Team & GDPR Champions	31/8/18	Green – in progress
GDPR 2				

Information You Hold				
2.1	**Information Asset Register** – to be completed with the assistance of GDPR Champions.	All Services/ GDPR Champions	7/5/18 - ASAP – this is the priority, as it will assist with Privacy Notices.	Green - Ongoing
2.2	**Data Minimisation** – all Services are to follow the Policy for the Retention and Disposal of Records Paper and Electronic to ensure that they hold the minimum data required.	ALL	25/518	Green - Ongoing
2.3	**Email data retention** communication to all staff and data purge to take place reducing the volume of legacy data held.	ICT & All Staff	25/5/18	Green – in progress
GDPR 3 **Communicating Privacy Information**				
3.1	**Privacy Notice** to be updated to reflect GDPR requirements and publish online.	Information Governance Team	18/5/18	Green – On track
3.2	**Privacy Notice Template and Guidance** issued to Champions.	Information Governance Team	4/5/18	Green - Template issued to GDPR Champions (March 2018). Guidance in draft form.
3.2	**Tailored Privacy Notices** Services to adapt tailored Privacy Notice to be used in their business and return for storing in the central repository online.	GDPR Champions	18/5/18	Green - Ongoing
3.3	**Communication Strategy** changes to public. This will be divided into legacy data (existing data), and new data. Consideration will be given to the mediums used to communicate whilst managing reputation and avoiding duplication across services.	Information Governance Team	18/5/18	Green - Ongoing
3.4	**Email footer** with link to corporate privacy notice for all staff including Councillors.	Information Governance Team	18/5/18	Green – in progress
GDPR 4 **Data Protection Impact Assessments**				

4.1	**Design Data Protection Impact Assessment and Guidance**	Information Governance Team	18/5/18	Green – in progress
GDPR 5 Contracts				
5.1	**Draft GDPR compliant contract clauses**	Information Governance Team/ Procurement and Legal	25/5/18	Green – in progress
GDPR 6 Data Sharing Agreements				
6.1	**Update Data Sharing Agreements**	Information Governance Team	25/5/18	Green – in progress