HAMPSHIRE COUNTY COUNCIL

Report

Committee:	Policy and Resources Select Committee
Date:	1 November 2018
Title:	Implementation of General Data Protection Regulation (GDPR) and Data Protection Act 2018
Report From:	Director of Transformation and Governance – Corporate Services

Contact name: Peter Andrews – Head of Risk and Information Governance,

Tel: 01962 847309 **Email:** peter.andrews@hants.gov.uk

1. Recommendation

1.1. That the Committee notes the contents of this report and that the County Council has the appropriate management systems, processes and procedures in place to meet the statutory requirements of GDPR and the associated Data Protection Act 2018.

2. Executive Summary

2.1. The purpose of this paper is to outline the key issues for the County Council arising from the implementation of the new General Data Protection Regulation (GDPR) and associated legislation in May 2018 and the actions taken to ensure that the County Council has met those requirements.

2.2. During the build up to the implementation of the new legislative requirements, the County Council undertook a comprehensive review of any changes needed and operated robust project management and governance procedures to ensure that any required changes were implemented in a timely and proportionate way.

2.3. The overall position is satisfactory, with all actions completed. Ongoing improvements have been identified as a consequence of GDPR implementation and are being actioned as business as usual.

2.4. The County Council has the appropriate management systems, processes and procedures in place to meet the statutory requirements of GDPR and the associated Data Protection Act 2018.

3. Contextual information

3.1. The General Data Protection Regulation (GDPR) and a new Data Protection Act replaced the previous law on May 25 2018. The use of technology has changed significantly since the original 1998 Data Protection Act came into force and the purpose of the new Regulation was to bring privacy legislation up to date, reflecting a world where personal data is collected more widely, and the risk of misusing data has increased.

3.2. As the Information Commissioner stated during the build up to GDPR implementation, “many of the GDPR’s main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under GDPR.”

3.3. The County Council was in a good starting position following the audit and subsequent report in January 2016 undertaken by the ICO, where the County Council had been awarded “High Assurance” status. Recent internal audits of Records Management and Information Governance had confirmed that the County Council already had in place much of the appropriate data protection measures in advance of GDPR.

3.4. The concept in GDPR of “privacy by design” is integral to how the County Council delivers services and handle individuals’ data. The County Council’s Information Governance Strategy sets standards that are entirely consistent with the requirements of GDPR and commits the County Council to ensuring that information is:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully.

3.5. Although the County Council started from a firm compliance base, the complexity of task undertaken across the organisation cannot be under estimated, not only because of the size and diversity of the personal information handled by the County Council, but also because much of the detailed guidance from the ICO was late in being produced; in fact the new Data Protection Act that contains much of the detailed requirements in English law was only passed by parliament days before GDPR implementation on 25 May.

4. Approach Taken

4.1. The County Council adopted the same framework for preparing for GDPR implementation as was successfully used to prepare for the ICO audit, with a clear project management approach and oversight from the Risk Management Board (RMB) and the oversight assistance of the Assistant Chief Executive and Chief Internal Auditor.

4.2. The RMB consists of Assistant and Deputy Directors from each department, who also undertake the role of Senior Information Risk Officer (SIRO) for each Department. They led and coordinated the work needed to bring the County Council to the necessary standard for GDPR, both collectively and for their respective Departments.

4.3. The frequency of RMB meetings was increased, with regular progress reports being received to the Board and the Corporate Management Team.

4.4. At an early stage the Information Law and Corporate Information Governance teams undertook a gap analysis to compare the County

Council's starting position against the requirements of the new legislation and a detailed corporate action plan was prepared.

4.5. In addition, Departments developed their own Departmental Delivery Plans to implement the changes that they needed to make, to compliment the corporate plan.

4.6. Departmental SIROs took the lead to identify and coordinate any changes to processes, systems and contracts affected by GDPR in their respective Departments.

4.7. In March 2018 the County Council's internal audit service, Southern Internal Audit Partnership, undertook a review of the preparations being made this provided assurance that the County Council was taking the appropriate steps to ensure that it complied with the requirements of GDPR, and endorsed the approach being taken.

5. **Key Areas of Change**

5.1. The County Council followed the ICO's 12 Recommended Steps approach to implementation of GDPR. The table attached to this report as Appendix 2 outlines the actions taken by the County Council in relation to those area.

6. Continuing steps

6.1. As with the introduction of any major legislation there is a period of refinement following the initial implementation, and this has been the case with the County Councils data protection arrangements. New guidance has been introduced and clarification received from the ICO and other bodies the County Council has made small changes to its documents as a consequence.

7. Conclusion

7.1. Following a comprehensive programme of preparation, the County Council has the appropriate management systems, processes and procedures in place to meet the statutory requirements of GDPR and the associated Data Protection Act 2018**.**

CORPORATE OR LEGAL INFORMATION:

Links to the Strategic Plan

Hampshire maintains strong and sustainable economic growth and prosperity:	yes
People in Hampshire live safe, healthy and independent lives:	yes
People in Hampshire enjoy a rich and diverse environment:	yes
People in Hampshire enjoy being part of strong, inclusive communities:	yes

Other Significant Links

Links to previous Member decisions:		
Title	Reference	Date
Direct links to specific legislation or Government Directives		
Title		Date

Section 100 D - Local Government Act 1972 - background documents

The following documents discuss facts or matters on which this report, or an important part of it, is based and have been relied upon to a material extent in the preparation of this report. (NB: the list excludes published works and any documents which disclose exempt or confidential information as defined in the Act.)

Document	Location
None	

IMPACT ASSESSMENTS:

1. Equality Duty

1.1. The County Council has a duty under Section 149 of the Equality Act 2010 ('the Act') to have due regard in the exercise of its functions to the need to:

Eliminate discrimination, harassment and victimisation and any other conduct prohibited under the Act;

Advance equality of opportunity between persons who share a relevant protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, gender and sexual orientation) and those who do not share it;

Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Due regard in this context involves having due regard in particular to:

1.1.1. The need to remove or minimise disadvantages suffered by persons sharing a relevant characteristic connected to that characteristic;

1.1.2. Take steps to meet the needs of persons sharing a relevant protected characteristic different from the needs of persons who do not share it;

1.1.3. Encourage persons sharing a relevant protected characteristic to participate in public life or in any other activity which participation by such persons is disproportionally low.

2. Equalities Impact Assessment:

As there are no proposed changes to the existing Policy a full Equalities Impact Assessment is not required, however potential impacts have been considered in the development of this report and no adverse impact has been identified.

Impact on Crime and Disorder:

The activities reported within this report have no effect on crime and disorder

Climate Change:

2.1.1. How does what is being proposed impact on our carbon footprint / energy consumption?

The activities reported within this report have no effect on climate change

2.1.2. How does what is being proposed consider the need to adapt to climate change, and be resilient to its longer term impacts?

The activities reported within this report have no effect on climate change.

12 Steps Recommended by the ICO	Actions Taken and Current Position
1. Awareness	GDPR training has been provided to all staff, through an e-learning training package and hard copy documents. In addition, a number of lunchtime learning and face to face training has been undertaken to individual teams across the County Council.
2. Information We Hold	A data-mapping exercise was undertaken based on a template provided by the ICO was undertaken. This identified the personal information that the County Council processes, along with the legal reasons for using that information.
3. Communicating privacy Information	The County Council already had a comprehensive suite of Privacy Notices that informed the public of the basis of that personal information was used. These notices were comprehensively reviewed and revised. The County Council holds a generic Privacy Notice that is published on its website. This outlines what personal information is used by the County Council and why. This supports local, more detailed Privacy Notices that are presented to the public when particular actions are undertaken, for example joining the library service or signing up to a newsletter. A separate Privacy Notice is in place that explains to staff the information the County Council processes as employer.
4. Individual's Rights	A number of additional rights were codified in GDPR, including the so called "right to be forgotten". The County Council introduced a number of processes to ensure that such requests are responded to in accordance with the requirements of the new legislation.
5. Subject Access Requests	Robust processes, with trained staff were already in place to facilitate citizen's requesting copies of the information held on them by the County Council. These were reviewed in light of shorter statutory timescales and the removal of the previous charging system.
6. Lawful Basis for Processing Personal Data	The County Council can only process personal information with a legal reason for such processing. The permitted legal reasons are outlined within GDPR. The legal reason will alter depending on the nature of the information being used, and the purpose for its use. The County Council has mapped where it processes personal information (in the Data Mapping exercise outlined above) and has identified the legal basis for processing that information across services provided by the County Council.

7. Consent	The GDPR introduced new requirements for the use and permissibility of using consent as a basis for processing personal information. In a number of cases this meant that asking for consent was no longer appropriate (as another legal basis for processing applied), in other areas, such as mailing lists, revised consent forms were produced, and new requests were sent to the relevant customers. However, this was undertaken in a proportionate way.
8. Children	The GDPR contains provisions intended to enhance the protection of children's personal data and to ensure that children are addressed in plain clear language that they can understand. A key part of the Action Plan undertaken by Children's Services involved reviewing the Privacy Notices used by Children's Services to take these changes into account.
9. Data Breaches	The GDPR introduced new stricter timescales for reporting serious data protection breaches to the ICO. The County Council has reviewed its data incident reporting and assessment process to streamline it and introduced a new assessment tool.
10. Data Protection by Design and Data Protection Impact Assessments	The GDPR introduced the overarching principle that data protection should be designed into any processes or use of personal information. Before any new IT systems or contracts that collect and use personal information are put in place a mandatory Data Protection Impact Assessment is undertaken. This looks at the implications that could arise from the processing personal information and requires data protection risks to be identified and mitigated.
11. Data Protection Officer	The County Council appointed its Monitoring Officer to undertake the role of Data Protection Officer, she is supported by the Head of Risk and Information Governance as Deputy Data Protection Officer.
12. International	This is relevant where the County Council may have suppliers processing information on its behalf outside the EEA, for example cloud-based services. Projects are subject to a Data Protection Impact Assessment that identifies any risks associated with information being processed abroad. In addition, all IT projects that involve cloud based services are subject to a rigorous security evaluation process.