Report to: **Cabinet**

Date of Meeting: **4th June 2018**

Report Title: **GDPR - Update**

Report By: **Chris Barkshire-Jones Chief Legal Officer and Monitoring Officer**

Purpose of Report

To up-date members on what steps have been taken in preparation for this legislation which came into force on the 25th May 2018. To seek Cabinet's approval of the following recommendations.

Recommendation(s)

1. To approve the Document Retention Policy.
2. To give the Chief Legal Officer delegated authority to amend the Document Retention Policy as necessary (in consultation with the Lead member) without bringing further reports to Cabinet.
3. Endorse the future development of an Information Management Strategy

Reasons for Recommendations

The GDPR came into effect on the 25th May 2018. As the Council processes data there are specific legal obligations that we must comply with.

Introduction

1. The General Data Protection Regulation 2014 came into effect on 25 May 2017. It applies to both personal data and sensitive personal data. The data protection principles set out the main responsibilities for organisations. These are similar to existing data protection law the most significant addition is the accountability principle. This requires organisations to show how they comply with the principles.

Information Commissioners Guidance

2. The Information Commissioner did prepare some early guidance giving organisations some idea as to what it needed to consider to comply with the legislation. The following are those bullet points and what we have done to comply with them.
3. Making key people and decision makers aware of the change in legislation is key. The Council has provided senior management with external training. It has provided some members with training (which is ongoing) and will ensure that all staff undertake mandatory e-training. The Chief Auditor will also consider the Corporate Strategic Risk register in light of GDPR
4. Organisations were advised to document what personal data they hold, where it came from and who we share it with. We have conducted a system/process audit with all services to understand this requirement. This has helped inform the Document Retention Policy and Privacy Assessments.
5. Organisations were advised to have effective policies and procedures in place to demonstrate how we comply with data protection principles. It is time that we consolidate policies on information developing them into an Information Management Strategy. This is work that needs to be undertaken as soon as possible but with an end date of 31st March 2019.
6. Every organisation needed to review their privacy notices. When you collect personal data you currently have to tell people how you intend to use their information. Additional requirements under GDPR are the need to explain your lawful process for processing the Data, your retention periods and that individuals have the right to complain to the Information Commissioner if they think there is a problem with the way we handle their data. We have undertaken a corporate 'umbrella' privacy notice with each service having their own privacy notice giving residents the required information.
7. Organisations are advised to check their procedures to ensure that we can ensure that individuals have the rights that they are entitled to. Some of these issues are around locating and destroying data. The Document Retention policy assists with this process. The policy gives practical advice on the need for officers to ensure that we are keeping data for the correct periods and ensuring that it is destroyed afterwards. This applies to any data whether held electronically or hard copy. The Chief Legal Officer and the Head of Information Technology are available to give advice.
8. The regulations on Subject Access Requests (SARS) have changed. In most cases we will not be able to administer a charge, Previously the fee was £10. We will only have a month to comply, previously it was 40 days. It is possible that this will significantly increase the workload. We will have to wait and see if this occurs.

9. Organisations need to identify the lawful basis for processing each activity, document it and include it in your privacy notices. As explained above we have conducted a data mapping exercise to capture this information which has been used to comply with the requirements of GDPR
10. Organisation were advised to re-visit how they seek, record and manage consent. It is not enough under GDPR to ask someone to tick a box to agree to consent. Consent must be expressly and freely given, specific, informed and unambiguous. There must be a positive opt-in. On application forms agreement to consent must be separate from other term and conditions. Meetings have taken place with some services to explain these requirements.
11. We need to ensure that we have the correct procedures in place to detect, report and investigate data breaches. This has been in place for some time.
12. We need to designate someone to take responsibility for data protection compliance and asses where this role will sit within the organisation.

LEGISLATIVE REQUIREMENTS - CONTRACTS

13. Articles 28-36 GDPR state that whenever a controller uses a processor the organisation needs to have a written contract in place. These contracts now need to include certain clauses as a minimum. All new contracts contain the clauses approved by the ICO. However, GDPR require that existing contracts need to have these clauses so we have undertaken a contract audit throughout the Council to ascertain which contracts these apply to. All applicable parties to those contracts have been contacted to ask for their written agreement to vary the existing contract to include the required GDPR clauses.

RIGHT TO COMPENSATION AND LIABILITY

14. Art 82 provides that any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. It is likely that the Courts will deal with this.

15. Administrative fines which are discretionary rather than mandatory there are two tiers applicable.

    i) Up to 10 million Euros or 2% of annual global turnover – whichever is the higher

    ii) Up to 20 million Euros or 4% of annual global turnover – whichever id the higher

    Infringements of the organisations obligations, including data security breaches will be subject to the lower level, whereas infringements of an individual's privacy rights will be subject to the higher level. The ICO must impose the fines on a case-by-case basis and must be 'effective, proportionate and dissuasive'

WORK TO CONTINUE – POST JUNE 2018

16. The ICO has yet to publish all the guidance relevant to GDPR. Once it has there may be other work to be undertaken. We know that we want to prepare a Management Information Strategy. It will be necessary to give staff training on how the Document Retention policy works and the practicalities of how to ensure that it is applied to both electronic information and hard copy. Furthermore, we

will need to ask staff to undertake an audit of existing information to determine whether it needs to be destroyed.

17. It is suggested that we review the whole process in May 2019.

Wards Affected

None

Implications

Relevant project tools applied? No

Please identify if this report contains any implications for the following:

Equalities and Community Cohesiveness
Crime and Fear of Crime (Section 17)
Risk Management
Environmental Issues
Economic/Financial Implications
Human Rights Act
Organisational Consequences
Local People's Views
Anti-Poverty

Additional Information

Appendix 1 Document Retention Policy

Officer to Contact

Officer Name Chris Barkshire-Jones
Officer Email Address cbarkshire-jones@hastings.gov.uk
Officer Telephone Number 01424 451731