(Informal Joint) Cabinet

St Edmundsbury BOROUGH COUNCIL

Title of Report:	**General Data Protection Regulations**	
Report No:	**CAB/SE/17/047**	
Report to and date:	**(Informal Joint) Cabinet**	10 October 2017
Portfolio holder:	Ian Houlder Portfolio Holder for Resources and Performance **Tel:** 01284 810074 **Email**: ian.houlder@stedsbc.gov.uk	
Lead officers:	Alex Wilson Director (and Senior Information Risk Owner) **Tel:** 01284 757695 **Email:** alex.wilson@westsuffolk.gov.uk Leah Mickleborough Service Manager, Democratic Services (and Monitoring Officer / Data Protection Officer) **Tel:** 01284 757162 **Email:** leah.mickleborough@westsuffolk.gov.uk	
Purpose of report:	The purpose of this report is to inform Cabinets of the forthcoming General Data Protection Regulations, and obtaining their support to the necessary action being taken to ensure the Councils are compliant with the new requirements.	
Recommendations:	**It is RECOMMENDED that Cabinet:** **(1) Supports the necessary action being taken to ensure compliance with the General Data Protection Regulations (GDPR), ensuring the Council continues to maintain high standards in the holding, keeping and maintenance of personal and sensitive data.** **(2) Approves a budget allocation of £80,000 to support compliance with GDPR, to be allocated on a 50:50 basis between the two West Suffolk Councils, as outlined in paragraph 2.5 of Report No: CAB/SE/17/047.**	

Key Decision: *(Check the appropriate box and delete all those that **do not** apply.)*	*Is this a Key Decision and, if so, under which definition?* Yes, it is a Key Decision - ☒ No, it is not a Key Decision - ☐ (a) A key decision means an executive decision which, pending any further guidance from the Secretary of State, is likely to: (ii) result in any new expenditure, income or savings of more than £50,000 in relation to the Council's revenue budget or capital programme.

*The decisions made as a result of this report will usually be published within **48 hours** and cannot be actioned until **five clear working days of the publication of the decision** have elapsed. This item is included on the Decisions Plan.*

Consultation:	This report has been subject to consultation with the Council's Information Governance Working Group
Alternative option(s):	GDPR is a legal requirement. As such, no other options have been considered.

Implications:

*Are there any **financial** implications? If yes, please give details*	Yes ☒ No ☐ • As identified within the report
*Are there any **staffing** implications? If yes, please give details*	Yes ☒ No ☐ • As identified within the report
*Are there any **ICT** implications? If yes, please give details*	Yes ☒ No ☐ • As identified within the report
*Are there any **legal and/or policy** implications? If yes, please give details*	Yes ☒ No ☐ • This report is required in order to comply with the GDPR
*Are there any **equality** implications? If yes, please give details*	Yes ☐ No ☒ • A screening opinion has been undertaken which did not identify any implications

Risk/opportunity assessment: *(potential hazards or opportunities affecting corporate, service or project objectives)*

Risk area	**Inherent level of risk** (before controls)	**Controls**	**Residual risk** (after controls)
Failure to implement GDPR leads to loss / mishandling of personal data and potential reputational damage, distress on the part of individuals and / or financial penalty	High	A comprehensive programme to implement GDPR is in development, with the aim of minimising risk associated with a potential data breach	Low

Ward(s) affected:	All wards
Background papers: *(all background papers are to be published on the website and a link included)*	None
Documents attached:	**Appendix 1:** key new requirements under GDPR

1. What is GDPR?

1.1 At present, Data Protection in the UK is governed by the Data Protection Act (DPA) 1998. On 25 May 2018, the General Data Protection Regulations (GDPR) will come into effect, and replace the Data Protection Act. Whilst the GDPR is EU law, the Government have made clear that the GDPR will apply within the UK after Brexit and as such, all organisations have to work to be compliant with GDPR ahead of the deadline.

1.2 Over the past 20 years, since the Data Protection Act came into force, the way that organisations deal with and process data has dramatically changed. The world has become increasingly digital, and as Councils, we have encouraged residents and partner organisations to work with us through electronic means; we also seek to share data – in a positive, yet secure way – with other organisations to improve the service and outcomes that our residents receive. Effective data management, that is compliant with the Data Protection Act, has become a normal part of our processes, systems and behaviour.

1.3 The GDPR seeks to provide a more modern framework for the handling of personal data, increasing the safeguards provided to individuals and improve their rights to access data held by organisations about them. Organisations that fail to comply, resulting in breaches in the way they handle data, could face significant financial penalty.

2. How is GDPR different to the Data Protection Act?

2.1 Appendix 1 outlines the key new requirements under GDPR, how these are different to the current Data Protection Act requirements, and how the Council is seeking to comply with these.

2.2 One of the most significant differences relates to the new requirement to report all data breaches which result in a risk to the "rights and freedoms" to individuals. As a result of breaches being reported, the Information Commissioner can issue fines, of a level up to 4% of turnover or 20m euros. This is a substantial increase to the current powers of the Information Commissioner, who is currently capped at issuing fines of £0.5m. Moreover, the Information Commissioner in future will be financed by fines issued for breaches in relevant legislation. At present, only a very small number of reported incidents result in a fine being issued. This change to the legislation could result in a greater number of fines being issued, at a higher financial penalty.

How is the Council responding?

2.3 In practice, several of the requirements will simply require modification to existing procedures, and ensuring that there is suitable training and promotion of these changes to support staff with compliance. However, there are some areas where substantial work will be required to identify the additional and necessary action required. For example, all Council procedures where personal data is processed have been developed to comply with the Data Protection Act; we will now need to review all such procedures

to assess whether or not they are compliant with the new requirements and if not, what action needs to be taken.

2.4 We are already working towards securing compliance in a number of areas. A data protection working group has been developed across Suffolk, in addition to the internal officer-led Information Governance Working Group which meets regularly to review all aspects of information governance compliance. An e-learning package is in development, in addition to other training and information being considered.

2.5 GDPR will inevitably impact upon almost all Council services and systems. In order to manage the programme effectively, additional resources are required to include recruitment of an additional project officer on a temporary basis (for one year), to provide for costs associated with provision and development of training, and to ensure support to the IT team for costs associated with the programme. With this in mind, a budgetary request is being made of £80,000 to support implementation costs; this will be allocated on a 50:50 basis between the two West Suffolk Councils and the s.151 Officer has confirmed that it will be feasible to fund this from existing budgetary underspends arising during the financial year.

2.6 At this stage, it is difficult to quantify the exact costs associated with compliance, as work may be required with systems providers and the project officer will need to work alongside services to undertake a detailed interrogation of processes to assess the extent of change required. This challenge is universal to all local authorities, and whilst it is hoped and expected that much of this work can be accommodated from existing budgets and resources, should additional significant resource implications arise this will necessarily follow relevant decision making routes.

3. What will this mean for Councillors?

3.1 Councillors will receive third party personal information in the course of undertaking their work through a variety of means. For example, they may receive e-mails from residents about issues that they face, that means acting as an advocate on behalf of the resident in talking to Council services.

3.2 When Councillors are in receipt of third party personal information, they are expected to be compliant with the Data Protection Act in the way they handle it – for example, ensuring they have the consent of the individual in talking to Council services or fellow ward Councillors about the resident's issues. Councillors will similarly be expected to comply with GDPR in future.

3.3 A number of safeguards already exist to help Councillors in their handling of personal data. All Councillors have to sign the Councils' Information Security Policy, which will be reviewed to ensure it is compliant with GDPR, and all Councillors receive data protection training periodically. Officers will be reviewing processes used by Councillors in dealing with the Council, and will ensure revised training and guidance is available to Councillors to aid them in their compliance under GDPR.

3.4 Councillors may also notice some physical changes in the way that information is presented at a Committee level, for example, being requested to consider Data Protection Impact Assessments where changes to systems / processes involve changes in the way that personal data is processed. Again, it is proposed that this will be included in training that will be provided to Councillors.

Appendix 1: GDPR versus the Data Protection Act

Requirement	How is this different to the Data Protection Act?	How will the Councils respond?
Accountability - As an organisation, we must put in robust governance arrangements over the management of personal data. Organisations have to actively demonstrate that they comply with GDPR.	Governance arrangements for personal data are inferred within the Data Protection Act, but are not a formal requirement.	In practice, the Council has implemented many parts of this "new" requirement – we have embedded data protection principles into policies and procedures. However, the GDPR programme will review each requirement and ensure necessary steps are taken to ensure full compliance.
Information Register – organisations must maintain a record of the data they hold, who is responsible for this data, and how the data is managed	This is a new requirement	The Council already maintains an information asset register which is subject to periodic updating.
Privacy Notices – when organisations obtain personal data, they should issue the subject with a notice explaining how their data will be processed and their rights	The Data Protection Act already requires the Councils to issue privacy notice. The GDPR is more explicit in what the notices must include, and requires the Council to provide more information	The Council will review all privacy notices currently used to ensure these are compliant with the new regulations
Subject Access – individuals have the rights to request access to the information organisations hold about them	Under the DPA, organisations had the right to charge £10 for such requests – the right to charge has been removed except where the request is unreasonable. The timeframes for responding have also been reduced, unless the request is very complex	Procedures for handling subject access requests will be reviewed and updated to ensure compliance with the new requirements.
Processing rights – there are various changes to the rights individuals have to influence the way their data is processed, for example individuals have the right to ask for their data to be removed and / or to prevent their data being processed. We can refuse in some circumstances –	The DPA only provided this right where processing the data would cause the individual distress or damage	The Councils will produce guidance, and develop and promote procedures, to comply with this element

for example, if we have to hold the data to comply with a legal duty		
Data Portability – individuals have the right to access data in a way that allows them to transfer their data from one environment to another	This is a new requirement	In practice, this may have limited applicability – for example, when a resident moves house and wishes to transfer data to another Council. However the Councils will produce guidance, and develop and promote procedures, to comply with this element
Consent – GDPR requires that an individual must have provided a freely given, specific, informed and unambiguous indication of their wish for their data to be used – i.e., they must have "opted in"; people must be able to easily withdraw consent. Organisations must demonstrate they have consent to use the data.	This is an enhanced requirement; before, use of "opt out" boxes was acceptable, although opt-in was preferred. The requirement to be able to demonstrate you hold consent is stricter than before.	Most organisations recognise this is a higher risk area for compliance. Whilst the Councils do not absolutely have to re-obtain consent from individuals, we have to be able to show any consent we hold is compliant with GDPR. This will require a review of the way that all personal data was collated, to assess whether that was compliant, and if not, may need to re-obtain consent to holding the data.
Childrens Data – GDPR introduces specific rules on the way that data about children is obtained and collated. In particular, there must be processes to verify the age of the child and obtain parental consent	This is a new requirement	The Councils have limited child-specific services. Where such services are identified, procedures will require review to ensure they are compliant.
Data Breach – all breaches which result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office. The Information Commissioner's Office have the power to issue fines (see below) where the breach identifies non-compliance with GDPR.	Although reporting of significant breaches is encouraged at present, there is no requirement to do so	The Council has procedures in place to review and report data breaches. These procedures will be reviewed to ensure compliance.
Data Protection Impact – assessments will need to be undertaken periodically to	This is a new requirement	The Council is building GDPR compliance into any new system procurements that

ensure our approach to data protection remains compliant. When we are making significant changes to the way that we handle or process data, we will be required to undertake a Data Protection Impact Assessment		involve the processing of personal data. Procedures will be developed to comply with the requirements.
Data Protection Officer – the Councils must appoint a Data Protection Officer who has sufficient knowledge and expertise of the organisation and data protection compliance	This is a new requirement	The Councils have historically appointed a Data Protection Officer, in a manner compliant with the regulations, and this will continue.
International Data requirements – data may only be transferred outside of the European Union where it is appropriate to do so	There are currently broadly similar requirements within the DPA	For example, there may be cases where third party suppliers host data on off-site servers outside of the EU. Council systems will be reviewed to ensure data capture and retention is compliant with this requirement.
Third Party Processing – if you are processing data on behalf of a third party, you will also be obliged to ensure processing principles are complied with, and you maintain appropriate security and record keeping in respect of the data	This is a new requirement – it is entirely the responsibility of the data controller to comply, not the third party processer at present	Where the Council processes data on behalf of third parties, processes need to be reviewed to ensure they are compliant with the new requirements. This may also require revisions to contracts and information sharing protocols.
Personal and Sensitive Data - the current definitions of personal and sensitive data have been clarified, but this also means that more data may need to be classified as personal	There are currently definitions, but the new rules are more specific which means we may need to look at more data being considered to be "in scope"	Review where we hold data which may now be considered to be personal and / or sensitive and ensure necessary requirements are being met (with respect obtaining consent and processing of data)
Compliance and Fines – should organisations fail to comply, maximum fines of 20m euros / 4% turnover can be enforced.	At present, the threshold for fines is £500k	n/a