TEWKESBURY BOROUGH COUNCIL

Report to:	Executive Committee
Date of Meeting:	7 June 2017
Subject:	Preparation for the General Data Protection Regulation
Report of:	Mike Dawson, Chief Executive
Corporate Lead:	Mike Dawson, Chief Executive
Lead Member:	Councillor D J Waters
Number of Appendices:	Two

Executive Summary:

This report summarises the impact on the Council of the new General Data Protection Regulation which comes into force on 25 May 2018 and the associated risks of non-compliance. The report gives details of steps taken to date and provides an initial action plan aimed at achieving compliance with the new requirements. Resource implications are dealt with, including proposals for a new post of Business Administration Manager to lead and coordinate work set out in the action plan and to maintain compliance post implementation of the new requirements.

Recommendation:

1) **That the Committee NOTES the action plan at Appendix 1 to achieve compliance with the General Data Protection Regulation.**
2) **That, subject to (3) below, the establishment of the Business Administration Manager's post is APPROVED in accordance with section 4 of this report.**
3) **That it be RECOMMENDED TO COUNCIL that the inclusion of the ongoing funding for the Business Administration Manager post be APPROVED for the base budget for 2018/19 and future years.**

Reasons for Recommendation:

To ensure the Council is compliant with the requirements of the General Data Protection Regulation.

Resource Implications:

The majority of the current work to achieve and maintain compliance with the General Data Protection Regulation can be undertaken within existing resources. A new post is proposed in section 4 of this report and the on-costed cost of that post is a maximum of £50,970. Provision has been made in the reserves list to fund the post during the current financial year, but ongoing provision is required in the Council's base budget for 2018/19 and beyond.

It is possible that there will be further resource implications as implementation works continue. This is especially likely in the area of ICT. Reports will be brought forward as required.

Legal Implications:

The Council is required to comply with new General Data Protection Regulation when it comes into force on 25 May 2018. The Information Commissioners Office has issued a guidance

checklist setting out actions required to achieve compliance by the implementation date. Compliance will need to be maintained post implementation and the Council may be subject to periodic inspection by the Information Commissioners Office. The new data protection framework brings new requirements and significantly increased fines for breaches. These are detailed in this report.

Risk Management Implications:

Non-compliance with the new data protection framework will expose the Council to reputational and financial risks. It may also give rise to poor handling of customer data which will undermine the customer service aims and objectives set out in the Council Plan. Fines for breaches of the new data protection framework can be as much as €20million.

An action plan has been developed to ensure timely implementation of work to improve data handling policies, procedures, systems and training. Implementation of this plan will be managed through the Council's project management programme and this will set out associated risks and mitigation measures.

Performance Management Follow-up:

The delivery of the action plan will be monitored through the project management system and Management Team at officer level. Reports in respect of progress will be forwarded to this Committee and the Overview and Scrutiny Committee as required. Ongoing audits of the data management system will be reported the Audit Committee.

Environmental Implications:

None.

1.0 INTRODUCTION/BACKGROUND

1.1 On 25 May 2018, the General Data Protection Regulation (GDPR) will come into force across the European Union (EU), replacing existing data protection laws. The GDPR will increase the rights of individuals over their personal data and tighten the obligations of all organisations to comply with new rules concerning the management of personal information.

1.2 While the UK decision to leave the EU means that the GDPR will no longer apply to the UK in the longer term, the GDPR will apply to the UK directly until the UK is no longer a member. Furthermore, the Government has confirmed that the UK will opt into the GDPR. Following this commitment, the UK Information Commissioner's Office (ICO) has stated that, whatever the outcome of the negotiations to exit the EU, UK data protection standards will be equivalent to the EU GDPR framework in order not to create any block on trade with the EU single market.

2.0 GDPR IMPACT ON THE COUNCIL

2.1 The Council handles and stores significant amounts of personal data as part of its routine service to its customers. The volume of data processed and retained is constantly increasing. Good data protection is therefore fundamental to high standards of customer service and the effective operation of the Council's business. Personal data is an asset owned by the customer as must be treated accordingly.

2.2 The GDPR significantly increases the data protection obligations on the Council and although existing data protection procedures are in place, these require extensive review and revision in order to achieve compliance with the GDPR framework.

2.3 Many of the GDPR's main concepts are the same as those in the current Data Protection Act 1998 (DPA). This means that the Council's current approach to compliance under

existing law will remain valid. However, new elements and significant enhancements within the GDPR will need to be taken account of and prepared for.

2.4 The most significant addition is a new 'accountability' requirement. Organisations, including the Council, will need to be able to demonstrate compliance with the GDPR principles, for example, by maintaining documentation on decisions about why personal information is being processed. Another important change is vastly increased fines for those organisations that fail to comply with GDPR or permit data breaches. For serious breaches organisations can be fined up to €20million. For less serious breaches or for failing to keep records the fine can be up to €10million.

2.5 To demonstrate compliance the Council must:

- Implement technical and organisational measures that demonstrate compliance. These include data protection policies, staff and Member training, internal data processing audits.
- Maintain relevant documentation on processing activities.
- Appoint a Data Protection Officer (DPO) (a new statutory role).
- Implement measures that meet the principles of data protection by design including, data minimisation, using artificial identifiers e.g. replacing a name with numbers and transparency.
- Implement data protection privacy impact assessments.

2.6 Under current DPA arrangements, the ICO only respond reactively to data breaches. It must be noted that, following implementation of the GDPR, the ICO will implement a proactive inspection regime to monitor compliance. Enforcement action could follow any breaches arising during inspections.

3.0 STEPS TAKEN TO DATE

3.1 The requirements of GDPR are extensive and complex.

3.2 The ICO has produced a checklist highlighting the specific steps that should be taken to meet the requirements of GDPR. This checklist has been used to develop an initial action plan to ensure compliance with GDPR by May 2018. As part of the programme it is planned to hold Member seminars on the GDPR impact and the implementation of policies and procedures to ensure the Council achieves compliance. The action plan is included at Appendix 1.

3.3 The action plan will require a significant amount of work to prepare for implementation. Following on from implementation there will be extensive ongoing work to manage the Council's data in compliance with GDPR requirements. This work will involve input from teams across the whole Council, but will require a dedicated resource to lead and coordinate the associated activities.

4.0 PROPOSED NEW BUSINESS ADMINISTRATION MANAGER POST

4.1 Given the extent, importance of the work and risks associated with achieving and importantly maintaining GDPR compliance, officers have considered the additional resources required. The specific functions required by the GDPR and existing data protection frameworks include the following roles:

- Senior Information Risk Owner (SIRO) – makes and is accountable for local risk management decisions e.g. Council use of cloud based services to store personal data etc.
- Data Controller (DC) – makes and is accountable for decisions on the purpose and use of personal data.
- Data Protection Officer (DPO) – advises monitors compliance and deals with the ICO.

4.2 The first two roles are already accommodated within the existing management resources, but the allocation of the roles to posts will be reviewed as part of the implementation action plan. The DPO role will be undertaken by One Legal and this can be accommodated within existing budgets.

4.3 In addition to the above, there is a need for a new post to work with the SIRO and DC and all teams to implement the requirements of GDPR and to maintain compliance post May 2018. The work involved is extensive and will involve all of the Council's administrative systems, both electronic and paper-based which process and store personal data. This will include processes from Customer Services through to the individual services themselves and require effective coordination of administration resources across the whole Council.

4.4 Given the requirements of the proposed new post it is suggested that it be established as a permanent post with the title of Business Administration Manager at Operational Manager/Team Leader level. The post will be located within Corporate Services Section of the Chief Executive's Unit reporting to the Corporate Services Manager. A draft job description and structure chart is attached for information at Appendix 2.

4.5 The Business Administration Manager role is subject to job evaluation, but it is anticipated that the post will be placed on scale H. The maximum annual cost of a scale H post is £50,970, including on-costs. Provision for the post in 2017/18 has been included in the reserves list within the Financial Outturn report elsewhere on this agenda. The cost of the post will need to be included in the base budget for 2018/19 and beyond and this will require approval by Council.

4.6 Given that the post is central to the timely implementation of work to prepare for GDPR compliance it is intended to recruit to the post as soon as possible following approval by the Executive Committee and Council at their June meetings. It is likely that the post will be filled internally which will allow for implementation work to be undertaken without delay.

5.0 OTHER OPTIONS CONSIDERED

5.1 None.

6.0 CONSULTATION

6.1 Consultation has been undertaken with the Leader of the Council as Lead Member for corporate governance.

7.0 RELEVANT COUNCIL POLICIES/STRATEGIES

7.1 Current data protection procedures.

8.0 RELEVANT GOVERNMENT POLICIES

8.1 GDPR Framework and ICO Guidance.

9.0 RESOURCE IMPLICATIONS (Human/Property)

9.1 The statutory roles required by the new GDPR Framework can be undertaken within existing resources; however a new post at operational manager level is required to coordinate and undertake work associated with the new requirements of the GDPR Framework.

10.0 SUSTAINABILITY IMPLICATIONS (Social/Community Safety/Cultural/ Economic/ Environment)

10.1 None.

11.0 IMPACT UPON (Value For Money/Equalities/E-Government/Human Rights/Health And Safety)

11.1 Data protection is a key area of the Council's work aimed at maintaining privacy which one of the rights listed in the Human Rights Act.

12.0 RELATED DECISIONS AND ANY OTHER RELEVANT FACTS

12.1 None.

Background Papers: None.

Contact Officer: Mike Dawson, Chief Executive Tel: 01684 272001

Email: mike.dawson@tewkesbury.gov.uk

Appendices:

1. GDPR Action Plan.
2. Draft Job Description – Business Administration Manager.