Committee:	Governance, Audit and Performance Committee	**Date:**	Thursday, 27 September 2018
Title:	General Data Protection Regulation (GDPR) Compliance Progress Report 27 September 2018		
Report Author:	Sheila Bronson, Audit Manager sbronson@uttlesford.gov.uk		

Summary

1. To provide an update to the Governance, Audit & Performance Committee details of work being undertaken by the Council's towards compliance with the EU General Data Protection Regulation (GDPR) and the UK's Data Protection Act 2018 (DPA 2018) which come into force on 25 May 2018

Recommendations

2. That the General Data Protection Regulation (GDPR) Compliance Progress Report be noted.

Financial Implications

3. None

Background Papers

4. None

Impact

5.

Communication/Consultation	An officer Project Team has been set up with representation from all departments
Community Safety	none
Equalities	None direct, although the need to protect sensitive personal data may be more significant for groups with one or more protected characteristics.
Health and Safety	none

Human Rights/Legal Implications	The Council is under a legal obligation to comply with the terms of the GDPR and DPA 2018 from 25 May 2018. Penalties can be imposed, and reputational damage suffered, if it does not. Non-compliance may also lead to an infringement of the rights of individuals, in particular their "Article 8" right to respect for their private life and home.
Sustainability	none
Ward-specific impacts	none
Workforce/Workplace	All Council employees need to be aware of data protection requirements and to carry out their work in a compliant manner. This is particularly important for employees who have access to sensitive personal information about members of the public

Situation

6. The EU General Data Protection Regulation (GDPR) and the UK's Data Protection Act 2018 (DPA 2108) came into force on 25 May 2018.

7. GDPR and DPA 2018 have replaced the Data Protection Act 1998.

8. The Council established a GDPR Project Team to undertake a programme of work to review the actions needed to work towards the Council's compliance with GDPR and DPA 2018 at 25 May 2018 and continuing compliance thereafter.

9. Two temporary posts (12 months) were created to oversee the GDPR compliance work; with the Internal Audit Manager appointed on secondment as GDPR Lead Officer from 01 August 2017 (the secondment has been extended to 31 October 2018) and a GDPR Compliance Officer in post from 13 November 2017.

Work Programme

10. The GDPR Project Plan included the actions needed to address the twelve steps identified by the Information Commissioner that organisations should take to ensure GDPR compliance

11. The GDPR Project Team with its revised membership of core Senior Managers will meet regularly until the end of December 2018 to review progress on the Project Plan; regular updates are also reported to the Corporate and Senior Management Teams. At the July meeting of the GDPR Project Team, Data Breaches; Subject Access Requests and Training were also reviewed.

12. A GDPR Compliance Progress Report will continue to be brought to future meetings of this committee during the lifetime of the GDPR Project. A copy of the current Project Plan is available to Members on request.

Progress to date

13. As of 25 May 2018, 48 out of the 54 tasks on the Project Plan had been completed; work is in progress on the remaining 6 tasks.

14. On-going compliance work from 25 May 2018 includes work on contract variations and data sharing agreements; further work on data held on systems; compilation of the Council's Information Asset Register & Record of Processing Activities and review and updating of the Council's Retention Policy and Schedules.

15. A compulsory GDPR training programme for all staff has been implemented and the programme of GDPR awareness for staff continues through the GDPR intranet page and news-letters.

16. Arrangements have been made for all UDC Councillors to have access to the Local Government Association's GDPR training course for councillors, although uptake has been limited to date.

17. Under the GDPR, it is mandatory for the Council as a public authority to appoint a Data Protection Officer (DPO). The GDPR specify the designation, position and tasks of the DPO along with the necessary level of expert knowledge. The GDPR Working Party 29 (WP29) Guidance recommends certain qualities and expertise that form a baseline that all appointed DPOs should meet:
    - Expertise in National and European data protection laws and practices, including an in-depth understanding of the GDPR;
    - Understanding of the processing operations carried out;
    - Understanding of information technologies and data security;
    - Knowledge of the business sector and the organisation;
    - Ability to promote a data protection culture within the organisation.

    and, depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:
    - Active support of the DPO function by senior management;
    - Sufficient time for the DPO to fulfil their tasks;
    - Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate;
    - Official communication of the designation of the DPO to all staff;
    - Access to other services within the organisation so that DPOs can receive essential support, input or information from those other services;
    - Continuous training.

18. Officers are considering permanent DPO arrangements after 31 October 2018 when the current arrangement of the Audit Manager as appointed interim DPO

working with the GDPR Compliance Officer on day to day DPO tasks will cease.

Risk Analysis

19.

Risk	Likelihood	Impact	Mitigating actions
The Information Commissioner can impose sanctions on the Council if it fails to show its compliance with GDPR from 25 May 2018	1 The Council did not achieve full compliance by 25 May 2018, however it can demonstrate the work it has undertaken towards full compliance	3 Data breeches due to non-compliance will be subject to sanctions varying in severity from warnings, reprimands, corrective orders to fines of up to €20m	Action is being taken to towards ensuring the Council is in a position to demonstrate continuing GDPR Compliance from 25 May 2018

1 = Little or no risk or impact
2 = Some risk or impact – action may be necessary.
3 = Significant risk or impact – action required
4 = Near certainty of risk occurring, catastrophic effect or failure of project.