APPENDIX 1

EXECUTIVE SUMMARY - ANNUAL INFORMATION GOVERNANCE REPORT

1. Introduction

1.1 The purpose of this report is to provide assurance to Governance, Audit and Performance Committee with regards to Data Protection and Information Governance matters that presently exists within the Council as of May 2020. A detailed report has been made to Corporate Management Team (CMT) who have approved the necessary operational actions that were required to be taken.

1.2 It is the intention to produce a report of this nature on a yearly basis both to CMT and also to committee to ensure they have ongoing assurance in relation to the Council's arrangements for Data Protection and Information Governance.

2. Background

2.1 It has now been two years since the European Union General Data Protection Regulations (GDPR) were first introduced within the United Kingdom. This led to the publication of the Data Protection Act 2018 which served to formalise and enhance GDPR and adopt it into UK legislation, The DPA 2018 was thereby given Royal Assent on the 25th May of that year.

2.2 The adoption of this new legislation provided the framework for the way personal data must always be processed and it became necessary for all organisations, (including Local Authorities) to conduct a review of their existing Data Protection policies and procedures and introduce a regime of new measures to ensure that they embarked on their journey towards becoming fully compliant with this new legislation.

2.3 GDPR introduced six (6) basic principles under which personal data should be processed and these principles would also ensure that greater accountability was observed by organisations wherever the processing of personal data was necessary. These principles are shown below:

Personal data must be

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and, where necessary, kept up to date;
- Retained only for as long as necessary;
- Processed in an appropriate manner to maintain security

2.4 Under the terms of GDPR the appointment of a Data Protection Officer (DPO) became a duty for all Public Authorities. The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. The role of the DPO and duties are as shown below:

- To inform and advise UDC and its employees about their obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws and with their data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- To advise on, and to monitor, data protection impact assessments;

- To cooperate with the supervisory authority; the Information Commissioners Office (ICO) and
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

2.5 The present DPO took up the post on 3rd January 2019, he regularly meets and works together with managers and officers throughout all service areas to continue to raise awareness of Data Protection matters and to advise all Council staff on their specific responsibilities as we continue on our path towards full compliance with the new Data Protection Act and GDPR.

2.6 A new suite of data protection policies and procedures were produced so that the Council complied with the requirements of GDPR. These documents were published on the UDC Intranet and staff were advised via the staff bulletin. In December 2018 however the GDPR tab was removed from the Councils Intranet which resulted in staff no longer having direct access and searching for GDPR and data protection policies became difficult to navigate and find what was required. This problem was identified during the recent Internal Audit of Information Governance conducted in February this year.

- Agreed action: CMT have directed that a GDPR / Data Protection folder containing all Policies and procedures should be included on the UDC Intranet with clear signposting for staff to navigate to find what they require.

3. Information Governance Group

3.1 One of the key areas which contributes towards the Council meeting our Data Protection responsibilities was the formation of a new Information Governance Group (IGG) and in June 2019 the inaugural meeting of this group took place. The group consists of several managers from those service areas who normally process high volumes of personal data. Representatives from Human Resources, Head of ICT department and the DPO are also members of this group.

3.2 The group exists for the purpose of safeguarding information assets throughout the Council and to provide a general oversight and support to the Council's Senior Information Risk Owner (SIRO) for all Information Governance matters. The group meets on a quarterly basis to discuss current Information Governance and Data Protection matters that have an impact within the Council. They report directly to both the Senior Information Risk Owner and to the Corporate Management Team on any issues which they consider could prevent the Council from meeting their legal compliance responsibilities. Minutes of each IGG meeting are circulated to CMT in the first instance and thereafter copied to members of the Senior Management Team so that the information can be used by service managers in cascade briefing to their teams.

3.3 The IGG's terms of reference are clearly defined however the group has yet to have an approved strategy framework document within which to operate. CMT have recommended that the strategy document should clearly outline the roles and lines of communication to both SIRO and Corporate Management Team and define specific responsibilities.

3.4 The IGG has been defined as a "Steering group" under their terms of reference as under normal circumstances they would refer important matters to CMT for decision.

The recent internal audit of Information Governance identified that the IGG identified that the IGG does not have the authority to direct or change policies or process**.**

- Action agreed; CMT have agreed that the IGG should remain a steering group and continue to report important issues which require a Corporate level decision to SIRO and the wider CMT.

UDC Levels of Performance

4. Data Breaches

4.1 On any given day Uttlesford District Council will deal with a considerable quantity of personal data for our customers, contractors, suppliers and staff. This data enables the Council to provide the full range of services to our local residents within the district and to meet our responsibilities as a District Authority. Our residents and those to whom we provide these services do expect their personal data to be managed securely and processed in a fair and appropriate manner and only for the purposes for which it was initially supplied to us.

4.2 Uttlesford District Council works hard to maintain its reputation as a safe custodian of our customer's personal data however sometimes mistakes can occur which may compromise the personal data we hold and certain information may regrettably be disclosed in error.

4.3 Any loss or disclosure of personal data within the control of the Council without prior approval or consent being given either by accident, negligence or deliberate act is considered to be a data breach. The official definition of a data breach is shown below:

"A breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to personal data. This includes breaches that are the result of both accidental and deliberate causes"

4.4 Any data breach that occurs within the Council is truly regrettable especially where it could have been avoided through staff taking more care and being fully aware of the potential risks that can occur when dealing with personal data. The consequences of any data breach to the person or persons most affected by the breach "the Data Subject(s)" can be significant and can often cause distress, anxiety and in some cases financial loss or result in theft of their identity and misrepresentation

4.5 Whenever a data breach has occurred and the circumstances involve a high risk to the rights and freedoms of the Data Subject(s) the Council is required to report the matter direct to the Information Commissioners Office within 72 hours. This report must outline the circumstances known at that stage and any actions the Council has taken to mitigate the risk of further loss. Any failure to follow this mandatory reporting procedure within the set timelines could result in the Council receiving a sanction from the ICO or in serious cases a hefty fine may be applied.

4.6 There are no significant concerns to report to members in relation to data breaches however CMT have agreed that the following measures should be introduced as a matter of course:

- Staff should be encouraged to report data breaches without fear of

disciplinary action being taken against them.

- Any change of address for residents should be updated on all management systems at the time of first notification

- Upon becoming aware of a data breach within their service area Managers must report the breach to the DPO as soon as practically possible

- A data breach report outlining the circumstances must be supplied to the DPO no later than 48 hours of the manager first being made aware of the data breach.

- DPO must conduct an impact assessment to establish the risks to the rights and freedoms of the data subjects affected and in serious cases report the circumstances as known at that stage to the ICO within the 72 hour timeline.

5. Subject Access Requests

5.1 Both GDPR and the new Data Protection Act 2018 gave data subjects far greater rights as to how their data should be processed and handled by organisations. These eight rights are as defined below:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

5.2 The right of access was particularly relevant for the Council to consider as this gave individuals the right to request their own personal data, (if held) and to receive this information in a suitable format of their choice within one month of the request being received. This process is referred to as a "Subject Access request (SAR).

5.3 Following the introduction of this new legislation the Council anticipated that a significant rise in requests from individuals seeking their own personal data would occur placing an additional administrative burden on staff. The expected rise in SAR requests has proven not to be the case however and although the administration involved in responding to each request is significant, it is nevertheless considered manageable within the current resources.

5.4 To date all Subject Access Requests received by the Council have been processed and actioned effectively within one month from the date of the Council first receiving the request as required under GDPR.

6 Freedom of Information & Environmental Information Regulations Requests

6.1 It is incumbent on the Council to be as open and transparent in all our business activities and to share information with our residents, customers and others whenever it is within our power to do so. The Council operates a publication scheme which follows the advice contained within the Ministry of Housing, Communities and Local

Governments paper "Local Government Transparency Code 2015." In complying with this code of practice the Council already publishes a great deal of information on how we spend our budget, the use of our assets, our decision making and other issues of interest to local people on our website as part of our commitment to comply with this code.

6.2 The Council does however receive a large quantity of other more diverse requests for specific information under either Freedom of Information Act 2000 or Environmental Information Regulations 2004. Under the terms of this legislation responses to requests are due within twenty (20) working days from the date we first received the request.

6.3 Table 1 below shows that the quantity of FOI's and EIR requests received by the Council has increased significantly over the last three years and is anticipated to continue to rise significantly above previous year's figures.

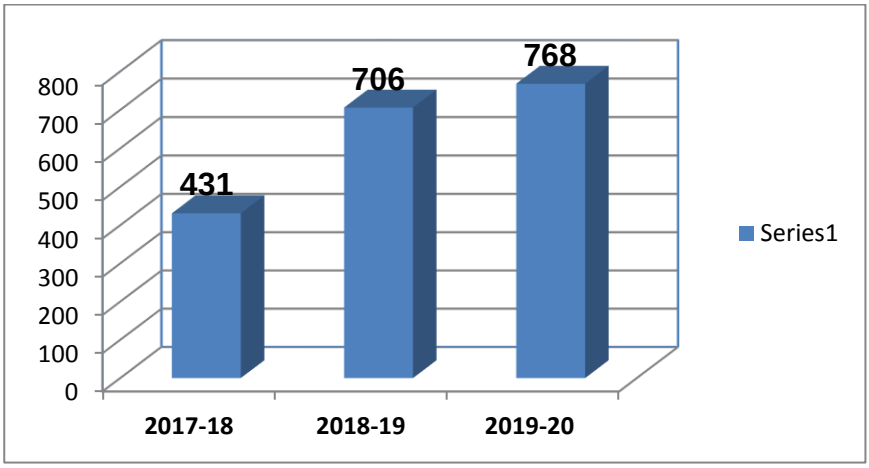

Table 1

6.4 Table 2 below highlights the number of requests received throughout last year by quarter, together with the time it has taken to provide a response. As can be seen, the Council supplied a response within the twenty (20) day timeline in nearly 70% of cases. Of some concern however is that over 20% of all requests received by the Council did not actually receive a response.

2019-20 - Responses	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	Total	%
No of requests received	**161**	**206**	**184**	**217**	**768**	
Within 20 Days	75	158	146	153	**532**	**69.27%**
More than 20 Days	24	17	16	13	**70**	**9.11%**
No response recorded	62	30	21	42	**155**	**20.18%**
Other reasons (i.e. Duplicated requests, Further clarity sought or withdrawn)	0	1	1	9	11	

Table 2

APPENDIX 1

6.5 To ensure we comply with FOI and EIR legislation in the way we manage these requests the Council operates a "Devolved approach." This means the requests are received centrally by a small team within the Legal Department consisting of the DPO and assisted by the Legal Assistant (Para-Legal). The FOI Team on receipt of the request record this on a bespoke Council Register then forward these onto the relevant service areas for officers to provide the response direct to the requestor in each case. The FOI team continue to track and monitor progress of the request from receipt to response as necessary.

6.6 This "devolved approach" of managing requests has the benefit of ensuring that the people with the most up to date knowledge are engaged in providing the response direct to the requestor. However the risk of applying this system is that the quality of the response can often be affected where officers are not dealing with FOI or EIR requests on a regular basis. Additionally officers can feel under pressure where their own duties are their main priority and the timeline for providing the response rapidly approaches the twenty (20) working day limit.

6.7 It was considered that the current devolved approach could be substantially improved if service areas select a small number of FOI liaison officers within their departments to take the lead role of dealing with FOI & EIR requests and for consulting with their service area colleagues to collate information relevant to the request. It was agreed that selected officers should receive some basic training from the DPO on the important issues to consider when handling requests.

6.8 In order to improve the Council's performance in this area CMT have approved the following actions which are in the process of being put in place:-

- In line with cabinet office guidance UDC should publish statistics of their responses to FOI and EIR requests on a quarterly basis
- Service managers should take ownership of FOI's EIR requests received within their service areas and ensure their officers provide a response in good time
- Service managers should elect FOI liaison officers to work alongside the FOI team and their own service area officers to ensure appropriate responses to requests are made within the approved timeline.
- DPO to provide training to selected Liaison officers to suitably prepare them for the new task to be undertaken.

Conclusion:

7.1 It is anticipated that the introduction of the measures approved by CMT will serve to further improve the way in which Information Governance is applied throughout the Council. Progress against these new measures will be reported regularly to CMT as part of the DPO's quarterly update.

T H Falconer
Data Protection Officer

August 2020