**Annex 1**

# Capital Plan Evaluation

| | | | | |
|---|---|---|---|---|
| | **Corporate : Information Technology Initiatives : General Data Protection Regulation (GDPR) Software** | | | |
| | 1 | **Specification**: | | |
| | | (i) | **Purpose of the scheme** | Software required to reduce risks under GDPR associated with the storage and access to unstructured data on Council IT Systems. |
| | | (ii) | **Relevance to National / Council's Objectives** | (a) National: EU General Data Protection Regulation (GDPR) 2018.<br>(b) Council:<br>• Alignment of GDPR compliance and data security policies.<br>• Mitigation of risk around data loss through preventative controls.<br>• Greater control and visibility of user access to data.<br>• Reduced storage costs through the identification of inactive data that can be removed.<br>• Improved efficiency gains within the helpdesk for maintaining user access controls. |
| | | (iii) | **Targets for judging success** | (a) Within the first three months:<br>• Identification of sensitive GDPR and PCI-DSS data across files shares.<br>• Identification of specific approved folders where sensitive data is permitted to be stored.<br>• Identify sensitive data outside of the approved folders, quarantine folders that are over 14 month old, monitor access to these areas and contact users who are accessing them.<br>• Understand who has access to the approved folders where sensitive data is permitted, and remove access for any users that are not permitted.<br>• Monitor for any new sensitive data being saved outside of the approved folders by scheduling and running regular reports.<br>(b) Milestones set at three month intervals to further refine and review the control of sensitive data. |

| | | |
|---|---|---|
| | 2 | **Description of Project / Design Issues:**<br>• One of the requirements of GDPR is to understand what data you hold and who has access to it.<br>• Structured data (such as that which is found in databases) is the most straightforward to understand since there will be a database schema containing a description of what data is stored, along with access controls and audit logs maintained by the systems administrators within departments.<br>• Updates to access controls in databases can be administered from a central location by the departmental system administrators using the tools within the relevant system (e.g. IDOX Uniform, Northgate iWorld, Capita Housing).<br>• Unstructured data (files and documents on network shares) prove more of a challenge. Locations such as the H and I drive contain folders that have various permutations of permissions allocated to them. Some can only be accessed by individuals, others by departmental teams, and some by the whole council.<br>• There is no overview of what the files on these folders contain. Some may be benign whilst others may contain sensitive personal information. Without manually inspecting each file individually it is not possible to catalogue the files to determine whether they pose a risk with regard to GDPR or other regulatory compliance regimes such as PCI-DSS.<br>• Using the standard tools available with Windows Server it is not possible to get an overview of access permissions across folders without manually inspecting each folder individually and noting the security permissions associated with it.<br>• Automated software is available which has the ability to identify the contents of files, categorise them on sensitivity, audit access permissions, audit file access and be able to report on its findings in an easily digestible form which can then be used by the software to update permissions automatically.<br>• This software can also assist with the management of users network accounts, identifying those that haven't been used for a long time, have expired passwords and those that have exceptions to the normal security profile / policy. |
| | 3 | **Milestones:**<br>The first three months after implementation establish a baseline of information stored, who has access to the data, and any risks associated with this information. Milestones are set at three month intervals to monitor the quarantine and removal of sensitive data from at risk locations.<br>**Risks:**<br>The use of this software assists with the mitigation of risk under GDPR under which the Information Commissioners Office (ICO) can impose fines of up to 20 million Euros or 4% of group worldwide turnover (whichever is greater) for non-compliance, breaches and incidents. |

4 **Consultation:**

- Members of the IT Services team have been consulted on the effectiveness of the product during a trial of the software conducted in February & March 2018.
- The Information Governance Officer Study Group has been consulted on the effectiveness of the software in assisting with the corporate GDPR delivery programme.
- Management Team have been consulted on how use of the software can mitigate risks associated with GDPR breaches and incidents.

5 **Capital Cost:**

The estimated capital cost of software is £66,000.

6 **Profiling of Expenditure:**

| 2018/19 (£’000) | 2019/20 (£’000) | 2020/21 (£’000) | 2021/22 (£’000) | 2022/23 (£’000) | 2023/24 (£’000) |
|---|---|---|---|---|---|
| **50** | **16** | | | | |

7 **Capital Renewals Impact:**

There is no impact on Capital Renewals. The annual support and maintenance agreement includes provision to keep the software up to date.

8 **Revenue Impact:**

Loss of investment Income at £3,000 per annum (based on £66,000 at 4%).  Annual support and maintenance for Year 1 at £20,000 and for year 2 and beyond £23,000 per annum.

9 **Partnership Funding:**

Not applicable.

<table>
<tr><td></td><td>10</td><td colspan="3"><b>Project Monitoring / Post Implementation Review</b>:<br>Scheme to be implemented by IT Services Manager.  Progress against the regular three monthly milestones will be provided to Management Team via the Information Governance OSG and reported to the Finance, Innovation and Property Advisory Board.  Post Implementation Review due 12 months after project completion.</td></tr>
<tr><td rowspan="5"></td><td rowspan="5">11</td><td colspan="3"><b>Screening for equality impacts:</b></td></tr>
<tr><td><b>Question</b></td><td><b>Answer</b></td><td><b>Explanation of impacts</b></td></tr>
<tr><td><b>a.</b> Does the decision being made or recommended through this paper have potential to cause adverse impact or discriminate against different groups in the community?</td><td>No</td><td></td></tr>
<tr><td><b>b.</b> Does the decision being made or recommended through this paper make a positive contribution to promoting equality?</td><td>No</td><td></td></tr>
<tr><td><b>c.</b> What steps are you taking to mitigate, reduce, avoid or minimise the impacts identified above?</td><td></td><td></td></tr>
<tr><td></td><td>12</td><td colspan="3"><b>Recommendation:</b><br>Scheme recommended for inclusion in the Capital Plan List A.</td></tr>
</table>