| Rushcliffe Borough Council | **Corporate Governance Group**<br><br>**10th May 2018**<br><br>**GDPR & ISO27001 Update** | **8** |
|---|---|---|

**Report of the Interim Chief Information Officer**

## 1. Summary

1.1 This paper deals with two separate but related matters:

- The Council's approach to implementing actions and changes in readiness for the General Data Protection Regulation (GDPR) on the 25th May 2018. The Council has made good progress in identifying, assessing and implementing the changes to meet its obligations associated with the new data protection legislation. More details of the work completed to date are provided below.
- Progress with and current status of a gap analysis of the Council's information management arrangements against the Information Security Management Standard ISO27001:2013. The gap analysis is still in progress but indicates the Council has managed systems in place across a number of control areas. Consideration is being given to applying for an external assessment to validate the internal analysis. More details of the work completed to date are provided below.

## 2. Recommendation

It is RECOMMENDED that the Corporate Governance Group note the contents of the report and the accompanying presentation.

## 3. General Data Protection Regulation (2016)

### Governance

3.1 The GDPR comes into effect on the 25th May 2018, and will be enacted in the UK through the Data Protection Act 2018. In November 2017 a formal GDPR Project Board was established, chaired by the Interim CIO, with support from the four Service Managers and ICT representation. An action plan was established based on the twelve work streams recommended by the Information Commissioners Office.

3.2 The Board has met regularly to assess progress and review and update the GDPR action plan. At the time of this report significant progress has been achieved and the action plan provides a framework for delivering and embedding further improvements relating to information management in general, and data protection in particular.

3.3 The current suite of Information & Security Management policies have been reviewed and updated and a number of new policies have been drafted, including a Data Protection Impact Assessment policy. A number of other corporate

templates, e.g. Project Management documents, have been reviewed and updated to reflect the changes associated with GDPR.

3.4 An internal audit conducted in February 2017 did not identify any significant weaknesses with the approach the Council was taking with respect to GDPR. The sections below provide further details on the twelve work streams within the action plan.

3.5 Awareness

A GDPR Communications Plan was implemented in late 2017. A new e-learning package was developed, tested and implemented and it is mandatory for all office-based staff to complete this training. At the time of this report 85% of staff had completed the training and active steps are being taken to ensure the remainder have done so no later than the 11th May. For field based staff a briefing session is planned for mid-May highlighting what GDPR means to them.

A new 'At a Glance' GDPR leaflet was produced and circulated to staff and Members during April. On-going communications via 'staff matters' have been issued, including a series of posters / screen savers, FAQs, a specific GDPR intranet page and electronic contact form.

A series of GDPR presentations have been delivered by the Interim CIO, including:

- Employee Liaison Group (December 2017);
- Leadership Forum (February 2018);
- Councillors Briefing (April 2018);
- Development Managers Liaison Group (April 2018);
- Town and Parish Councillors Forum (May 2018)
- Leadership Forum (booked for 17th May 2018)

3.6 Information the Council holds

The Council reviewed and updated its existing Information Asset Register (IAR) to ensure it captured all of the requirements of GDPR. All Information Asset Owners (IAOs, typically Lead Specialists) engaged with the process of updating their IAR. Actions arising from this update, for example, identifying where a data sharing agreement is required, are being addressed as part of the CIO Work programme for 2018/19.

3.7 Communicating Privacy Information

As part of the update of the IAR, identifying opportunities to introduce, change or replace existing or new privacy notices were identified. Under GDPR, privacy notices need to be more comprehensive and explicit when informing the public about how the Council will manage and protect their personal and sensitive information. A number of privacy notice templates have been created and are being implemented with the IAOs.

3.8 Individual's Rights

The implementation of GDPR introduces enhanced rights for citizens, otherwise known as 'data subjects'. The Council has been reviewing how current systems

enable these rights to be exercised, e.g. through the provision of an appropriate privacy notice.

3.9 Subject Access Requests

GDPR introduces two notable changes compared to the current subject access rights under the Data Protection Act (1998):

- A reduced time limit to respond to such requests - 30 calendar days rather than 40;
- In most cases, a standard £10 charge to process such requests cannot be charged.

Historically, the Council's Senior Solicitor has dealt with subject access requests and the number of requests has generally been low. Since the retirement of the Senior Solicitor in April 2018 other members of the Legal Services team have assumed interim ownership of any submitted requests.

A new Subject Access Request policy has been drafted along with a new range of supporting procedures, notices and template letters.

3.10 Legal Basis for Processing Personal Data

Through the updates to the IAR, each personal data process or flow has identified the legal basis underpinning that process or flow. In cases where the process or flow involves a third party acting as a 'data processor', proactive engagement has taken place to ensure the Council obtains written assurances that these providers are themselves GDPR ready. The contracts management arrangement and systems are being updated to provide a robust framework for the future, at all stages of the contract lifecycle.

Where the IAR has indicated the requirement for a formal contract or data sharing/processing agreement, these are being addressed as part of on-going work. New data sharing and data processing templates have been created and are now being implemented as part of a phased roll-out.

3.11 Consent

The updates to the IAR have identified a small number of personal data processes or flows which rely on consent as the legal basis for data processing. Work is underway with the relevant IAOs to ensure this processing is underpinned by robust systems for capturing and recording consent, for reviewing these consents on a regular basis and for acting on instructions where consent is withdrawn.

In February 2017, the RCCC changed its processes to include the ability for members of the public who had contacted them to provide their consent to receive official information from the Council about matters of general interest. By the end of April, approximately 2400 citizens had provided this consent and work is underway to agree how to utilise this information to keep local residents informed and up to date (in a cost effective manner) about activities the Council is organising or facilitating.

3.12 Children

Under GDPR, 'children' are defined as anyone under 16. The UK has applied a derogation which reduces this to 13. The main effect of this is to enable UK citizens aged 13 and above the legal right to provide their own consent rather than having to obtain this from their parents or other legal guardian. Particular care relating to the management of children's personal data (including the ability to verify the actual age of the child) is required where they may be accessing or using 'information society services' such as social networking platforms.

To date, this has not been identified as a significant issue for the Council but this is being kept under review as part of on-going work.

3.13 Data Breaches

One of the biggest areas of impact arising from GDPR is the additional requirements and responsibilities in the event of a personal data breach. The scope of what needs to be captured and reported, internally and externally, represents a marked change to the current reporting regime. Third party data processors are also impacted by these changes. The penalties and fines under GDPR are significantly higher than under DPA (1998).

The Information Commissioners Office (ICO) has published guidance on the management of personal data breaches and the Council is applying this guidance to update of our internal policy. A desktop 'breach incident' exercise is planned for May.

3.14 Data Protection by Design (DPbD) & Data Protection Impact Assessments (DPIA)

Previously recommended as good practice, DPbD and DPIAs are now enshrined as part of GDPR. The Council has carried out Privacy Impact Assessments in the past but there will be higher expectations to ensure both DPbD and DPIA are incorporated into project governance and change management arrangements going forward.

A specific policy has been drafted to address this requirement and project management templates are being updated. The Interim CIO will be attending the Leadership Forum on the 17th May to give the EMT, Service Managers and Lead Specialists a presentation on this particular area of change associated with data protection.

3.15 Data Protection Officer (DPO)

As a public authority the Council is legally required to have a DPO in post as part of the GDPR accountability framework. The Interim CIO is the designated DPO (and SIRO) at the current time. It is anticipated this responsibility will revert back to the substantive CIO in late July / early August.

To embed this role within the Council, the roles and responsibilities of the DPO have been reflected in the policy review process and the 'Guidance on Mandatory Roles' training document aimed at Lead Specialists and above.

The SIRO Audit template has also been updated to include additional questions to reflect GDPR. This audit is underway and the outputs and actions arising will be reported to EMT and form part of the DPO work programme for 2018/19.

The designation, position and tasks of the DPO (as described in GDPR Articles 37-39) will be kept under review going forward to ensure the requirements of the role continue to be met.

3.16 International

This relates to organisations who operate internationally so does not apply to the Council. Through the updates to the IAR we have confirmed that there are no international data transfers in place. This issue will be kept under review as part of the maintenance of the IARs.

**ISO27001: 2013 Gap Analysis**

3.17 The Council has, for a period of time, been tracking its compliance against ISO27001 ("the standard") as part of the information management strategy and related policies. More recently, the Council achieved certification against the Cyber Essentials standard which is comprised of a smaller set of security control objectives. A recent 'Cyber Security and ISO27001' internal audit report highlighted six low priority recommendations which will be fed into further improvement activities.

3.18 The standard is generally regarded as a more comprehensive set of controls, covering not just technical controls but addressing related areas such as physical security, human resources, training, information classification, supplier management and compliance with legal and contractual requirements. In some respects, therefore, there are overlaps with GDPR and it is already clear that progress made with the latter, e.g. in relation to the management and due diligence around ICT systems and supplier contracts, is having a positive impact on some control areas within the standard.

3.19 Certification against the standard is considered as the benchmark for any organisation seeking to obtain independent assurance that its own control environment is robust. It is also a *de facto* requirement for organisations offering a commercial, professional ICT service to others and is increasingly becoming essential if an organisation is applying for government or other public sector contracts, especially where personal or sensitive data is involved.

3.20 A gap analysis against the standard is in progress. The scope of the analysis is the ICT team and systems. Two meetings have taken place with the ICT Manager and wider team (February and April) to review each control objective in turn. When deciding on the status, reference was made to the auditing guidelines published by the ISO27k Forum.

3.21 For each control objective an assessment was made using the criteria below. The number of requirements in each category indicated:

| | | |
|---|---|---|
| N/A | Not Applicable | 4 |
| Initial (Red) | Development has barely started and will require significant work to fulfil the requirements | 3 |
| Defined | Development is more or less complete although detail is | 26 |

| | | |
|---|---|---|
| (Amber) | lacking and/or it is not yet implemented, enforced and actively supported by top management | |
| Managed (Green) | Development is complete, the process/control has been implemented and recently started operating | 81 |
| | Total | 114 |

3.22 During May-June the gap analysis will be developed further. A separate ISMS document will be developed, cross-referencing individual policies and procedures already in place, and encapsulating the wider security governance arrangements relevant to the standard. Active consideration is being given to the introduction of a subset of security metrics derived from ISO27004/2016 to provide security management indicators in support of specific control objectives related to the standard. These will be agreed and implemented during this same time period.

3.23 Two external organisations have provided a non-binding quote to carry out an external assessment against the standard, using the ISMS and gap analysis completed internally, along with a separate on-site visit. This will cost approximately £1000 and could be completed before the end of July 2018.

3.24 The Council has been following many aspects of the standard over recent years. The gap analysis to date suggests that this has led to a level of maturity which would stand the Council in good stead if it were to apply for certification. At the very least, the gap analysis has identified a number of improvement opportunities that are being progressed with the ICT team.

3.25 If certification was sought and achieved, this external and independent endorsement would demonstrate high standards and a professional approach to ICT management which could be a valuable selling point as the Council seeks further commercialisation opportunities in the future.

## 4. Standards

4.1 **Appendix A** lists a number of standards that the Council is either certified against or maintains compliance with. Certain standards incur cost to achieve certification; as a result, a decision is made whether to simply maintain compliance with a standard or whether to invest funds to achieve certification.

## 5. Implications

### 5.1 Finance

Dependent on approval, the Council may commit to obtaining an external assessment against the ISO27001 standard within the next three months. The costs received to date indicate this will be in the region of £1000. Costs associated with the changes relating to GDPR are being met within existing resources.

### 5.2 Legal

The Council needs to abide by the requirements of the Freedom of Information and Data Protection Acts. The Council is obligated to look after data and sensitive data in the appropriate way. If a member of the public is unhappy with the way his or her data has been handled they can make a complaint to the Council or to the Information Commissioner.

5.3 **Corporate Priorities**

The implementation of the requirements associated with GDPR aligns with and supports the Council's Corporate Priorities. Achieving certification against ISO27001 would further strengthen and underpin the general responsibility for the Council to demonstrate it has a robust information security and governance framework in place, and could further contribute to achieving future commercialisation income.

5.4 **Other implications**

There are no other implications.

| | |
|---|---|
| **For more information contact:** | Ken Thompson<br>Interim Chief Information Officer<br>07817 319431<br>kthompson@rushcliffe.gov.uk |
| **Background papers Available for Inspection:** | GDPR Project Board Terms of Reference, Minutes and Action Plan<br>GDPR Communications Plan<br>ISO27001 Gap Analysis assessment |
| **List of appendices (if any):** | Appendix A – Glossary of terms / standards |

**Appendix A**

## Glossary of terms / standards

| | |
|---|---|
| **CoCo** | Code of connection – the standards that must be met in order for a local authority to be connected to the Public Services Network (PSN). Currently provides for example secure email and access to Department of Work and Pensions data to support the Council's processing of Housing Benefits.<br>**(The Council is certified against this standard)** |
| **Cyber Essentials** | Is a UK government scheme encouraging organisations to adopt good practice in information security. It includes an assurance framework and a simple set of security controls to protect information from threats coming from the internet.<br>**(The Council achieved certification against this standard in February 2018)** |
| **GDPR** | General Data Protection Regulation, which will be enacted in the UK through the Data Protection Act 2018.<br>**(The Council is compliant with its legal responsibilities as a Data Controller)** |
| **ISO 27001** | Is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.<br>**(The Council aims to remain compliant with this standard as a minimum, and seek external assessment in 2018)** |
| **PCI/DSS** | Payment Card Industry - Data Security Standards. The Council must be compliant with this set of standards in order to enable it to process payments made using credit or debit cards.<br>**(The Council is certified against this standard)** |
| **PSN** | Public Services Network.<br>**(The Council is certified against this standard)** |