Rotherham Metropolitan Borough Council

Public Report
Audit Committee

Committee Name and Date of Committee Meeting
Audit Committee – 26 November 2019

Report Title
IG/GDPR Annual Report 2018/19

Is this a Key Decision and has it been included on the Forward Plan?
No, but it has been included on the Forward Plan

Strategic Director Approving Submission of the Report
Judith Badger, Strategic Director of Finance and Customer Services

Report Author(s)
Luke Sayers, Assistant Director- Customer, Information and Digital Services
luke.sayers@rotherham.gov.uk

Paul Vessey, Head of Information Management
paul.vessey@rotherham.gov.uk

Ward(s) Affected
Borough-Wide

Report Summary
This report is an update and annual report on the council's compliance with the General Data Protection Regulation and the Data Protection Act.

Recommendations
The Audit Committee is asked to:-

1. Note the production of the GDPR Annual Report 2018/19.

2. Note that it is legal requirement that the council continues its maintenance of its Information Governance policies and processes in compliance with legislation.

List of Appendices Included
Appendix 1 GDPR Compliance Summary of Outstanding Tasks
Appendix 2 FOI & RoAR Statistics

Background Papers
Information Commissioner's Office
https://ico.org.uk/

A-Z of Information Management Documents
http://rmbcintranet/Directorates/FCS/CIDS/IM/Pages/A-Z_of_Documents.aspx

Consideration by any other Council Committee, Scrutiny or Advisory Panel
No

Council Approval Required
No

Exempt from the Press and Public
No

Error! Reference source not found.

1. Background

1.1 This report is an update and annual report on the council's progress towards full compliance with General Data Protection Regulation and the Data Protection Act.

1.2 The General Data Protection Regulation (EU) 2016/679 (GDPR) sets out the key principles, rights and obligations for processing of personal data. The GDPR came into effect on 25 May 2018. As a European Regulation, it has direct effect in UK law and automatically applies in the UK.

1.3 The Data Protection Act 2018 (DPA) sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It sits alongside the GDPR, and tailors how the GDPR applies in the UK - for example by providing exemptions. It also sets out the Information Commissioner's functions and powers.

1.4 The Information Commissioners Office is the UK's independent body set up to uphold information rights and it is responsible for enforcement of the rights and responsibilities set out in the GDPR and DPA.

1.5 A council-wide project reviewed the council's approach to data protection and ensured its governance and information management processes and policies fully complied with the requirements of GDPR and DPA.

1.6 The Audit Committee last received an update on the project's progress in June 2018 and, for completeness, Appendix 1 provides the list of outstanding tasks that were presented to the committee.

1.7 All outstanding tasks have since been completed and all required policies and processes for compliance with GDPR and DPA are now in place and embedded within the organisation.

1.8 Now that all the elements are in place, it is the responsibility of all directorates and service areas to comply with the council's data protection policies and procedures.

1.9 Monitoring of the council's compliance with GDPR and DPA is carried out by the Corporate Information Governance Group (CIGG) which has representatives from all Directorates and is chaired by the Council's Senior Information Risk Officer.

1.10 Any risks relating to Information Governance, including GDPR and Data Protection are monitored on a regular basis by this group. Risks and actions are logged and reviewed at CIGG meetings and, if necessary, are escalated in line with the Council's risk management processes.

2. Key Issues

2.1 Maintain Compliance:

2.1.1 The key issue is to ensure that compliance with data protection legislation is maintained.

2.1.2 Compliance with Data Protection principles is a continuous project and CIGG fulfils a core function in monitoring and overseeing information risks and in regularly monitoring the effectiveness of the council's Data Protection policies and each directorate's information governance and data protection processes.

2.2 Raised Awareness of Data Protection:

2.2.1 Due to improvements in employee training awareness, there has been an increase in the identification of potential risks and a consequential improvement in processes.

2.2.2 Similarly, public awareness of information rights has also resulted in an increase of 75% in the volume of right of access requests (RoARs).

2.2.3 The council received 97 RoARs in financial year 17/18 and 170 requests during financial year 18/19. The volume for 19/20 will be monitored for any trend.

2.3 Monitor Performance of Freedom of Information and Right of Access Requests:

2.3.1 Completion times for both types of requests have seen improved performance despite a significant increase in the volume of enquiries. Appendix 2 provides performance for the last three financial years.

2.3.2 Performance will continue to be closely monitored with the focus on further improvement.

2.3.3 One key issue is that requests vary substantially in complexity and workload making analysing, allocating resources and forecasting problematic.

3. Options considered and recommended proposal

3.1 There are no new proposals or recommended options. However it is a requirement that the council continues the maintenance of its Information Governance policies and processes in compliance with Data Protection requirements.

3.2 It should be noted that continued compliance to GDPR and the Data Protection Act 2018 can only be achieved by the continued support of all Council Staff and Councillors. Key roles such as Information Asset Owners and Data Protection Officer can use existing governance structures to ensure on going compliance.

4. Consultation on proposal

4.1 None

5. Timetable and Accountability for Implementing this Decision

5.1 None

6. Financial and Procurement Advice and Implications (to be written by the relevant Head of Finance and the Head of Procurement on behalf of s151 Officer)

6.1 There are no direct financial or procurement implications arising from this report.

7. Legal Advice and Implications (to be written by Legal Officer on behalf of Assistant Director Legal Services)

7.1 There are no legal implications arising from this report, except to reiterate that the council has a duty to comply with Data Protection legislation.

8. Human Resources Advice and Implications

8.1 There are no direct implications for HR arising from this report.

9. Implications for Children and Young People and Vulnerable Adults

9.1 There are no direct implications for children and young people or vulnerable adults arising from this report.

10. Equalities and Human Rights Advice and Implications

10.1 There are no direct equalities or human rights implications arising from this report.

11. Implications for Partners

11.1 There are no direct implications for partners arising from this report.

12. Risks and Mitigation

12.1 Risks and mitigation will be managed by CIGG and the council's risk processes.

13. Accountable Officer(s)

Luke Sayers, Assistant Director- Customer, Information and Digital Services
luke.sayers@rotherham.gov.uk

Paul Vessey, Head of Information Management
paul.vessey@rotherham.gov.uk

Approvals obtained on behalf of:-

	Named Officer	Date
Chief Executive		Click here to enter a date.
Strategic Director of Finance & Customer Services (S.151 Officer)	Named officer	Click here to enter a date.
Assistant Director of Legal Services (Monitoring Officer)	Named officer	Click here to enter a date.
Assistant Director of Human Resources (if appropriate)		Click here to enter a date.
Head of Human Resources (if appropriate)		Click here to enter a date.

Report Author:
Luke Sayers, Assistant Director- Customer, Information and Digital Services
luke.sayers@rotherham.gov.uk

Paul Vessey, Head of Information Management
paul.vessey@rotherham.gov.uk

This report is published on the Council's website.

Appendix 1: GDPR Compliance Summary of Outstanding Tasks

Phase 1 (Mar-Jul 17): Raise Awareness, Build Accountability and Gather Information

1.5 Carry out a review of IT systems and procedures in light of new information rights, to include:

Deliverables outstanding in last report:

- List of risks across RMBC high risk systems in relation to GDPR compliance - completed

- Digital solutions agreed between System Owners and Software Suppliers to meet GDPR compliance e.g. right to erasure, portability - completed

- Offline solutions agreed with System Owners to meet GDPR compliance - completed

Status: **Closed**

1.6 Review the resource and training requirements within the IM Team, to include:

Deliverables outstanding in last report::

- GDPR Training for IM Team ongoing – completed

Status: **Closed**

Phase 2: Plan and Prioritise (Jul – Nov 17)

2.1 Recruit and appoint a Data Protection Officer (DPO):

Deliverables outstanding in last report:

- DPO not yet formally appointed - completed

Status: **Closed**

2.2 Prioritise compliance activity and remedial measures based on areas with high risk and most significant impact (identified via Information Audit and Information Rights Review)

Deliverables outstanding in last report:

- Risk assessments outstanding for 2 IAO's due to delays within services completing the Information Audit - completed

- Improvement plans outstanding for 2 IAO's due to delays within services completing the Information Audit - completed

- Directorate resource to be allocated to the improvement plan deliverables - completed

- A monitoring and review schedule to be agreed between the IAO and IM Team to complete improvement Plans- completed

- All Information risks will not be mitigated by May 2018 due to the delays in completing the Information Audit - completed

Status: **Closed**

2.3 Embed Privacy Impact Assessment (PIA) guidance and process across the Council

Deliverables outstanding in last report:

- PIA Checklist Template to be updated to reflect GDPR requirements - completed

Status: **Closed**

2.4 Conduct retrospective PIA's for riskier activities
Deliverables outstanding in last report:
- PIA's outstanding for 75% of CCTV systems - completed
- PIA's to be completed for cloud based systems - completed

Status: **Closed**

2.5 Embed the data breach guidance and process across the Council
Deliverables achieved:
-Deliverables outstanding in last report
- Communicate across the Council, tighter reporting deadlines e.g. 72 hours - completed

Status: **Closed**

Phase 3: Implement Changes (Dec17-Apr 18, 5 months)

3.1 Review and update privacy standards and processes
Deliverables outstanding in last report:
- Finalised and approved Directorate Privacy Notices to be uploaded to the external site - completed

Status: **Closed**

3.2 Review and update consent standards and processes
Deliverables outstanding in last report:
- IAO to review the lawful basis for processing personal data (6 bases) where the information audit has identified reliance on 'consent'. Local Authorities should be reliant on public task when processing personal data, consent only on an exception basis. - completed

Status: **Closed**

3.3 Review and update information sharing (inc. confidentiality) standards and processes
Deliverables outstanding:
- The Council is able to monitor compliance by maintaining a central register of information sharing agreements in readiness for the regional information gateway project - completed

Status: **Closed**

3.4 Review and update information rights standards and processes
Deliverables outstanding:
- The Council has a tested process for each information right -completed
- The Council is able to monitor compliance against legislation and report KPI's to CIGG on a monthly basis - completed

Status: **Closed**

3.5 Review commissioning supply chain and update contracts in line with GDPR requirements
Deliverables outstanding:
- Legacy contracts revised - completed
- New contracts incorporate contract clause- completed

Status: **Closed**

Phase 4: Embed change, train and re-train (May-Jul 18, 3 months)

4.1 Implement the appropriate standards and processes in order to embed culture change

Deliverables achieved:

- New Information Management intranet site developed which incorporates GDPR standards and processes
- Internet site prepared ready for launch which incorporates GDPR guidance

Deliverables outstanding:

- Demonstrate compliance with all obligations under the GDPR through the Councils completed Information Asset Register - completed
- Demonstrate standards and processes used to embed cultural change via digital communications (internet/intranet) - completed

Status: **Closed**

4.2 Implement an appropriate training plan in order to embed culture change

Deliverables achieved:

- SIRO/IAO/CG Training by Act Now 23/5/17
- e-learning module available to all accessing the Council's network
- GDPR video's x 2 embedded within the Council's e-learning system ready for launch in Apr 2018 subject to technical testing

Deliverables outstanding:

- Pre GDPR training material launched - completed
- Post GDPR training material launched - completed

Status: **Closed**

4.3 Implement the Communication Plan in order to embed culture change

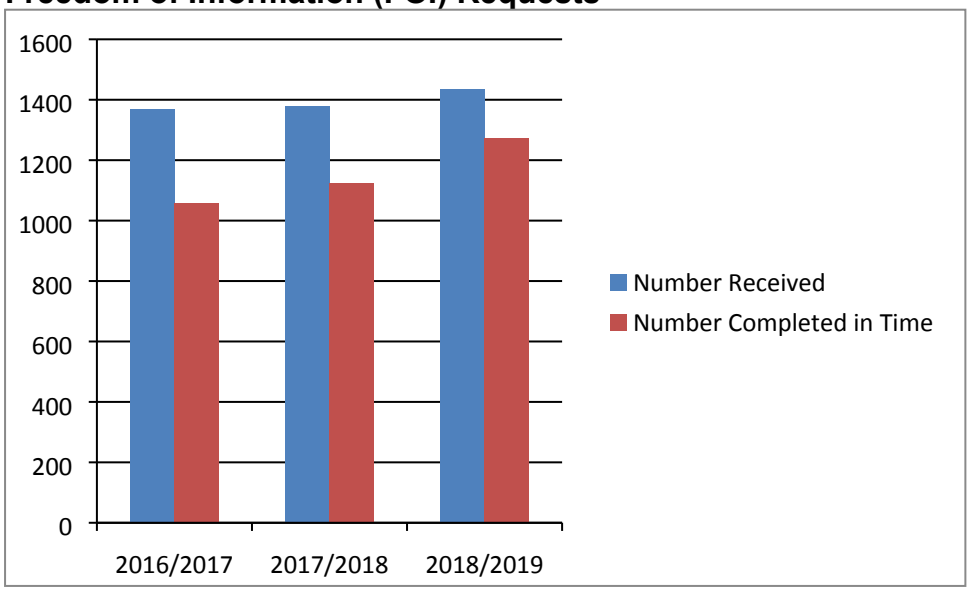
Deliverables outstanding:

- Development of a Communication Strategy which is effective in embedding cultural change - completed

Status: **Closed**

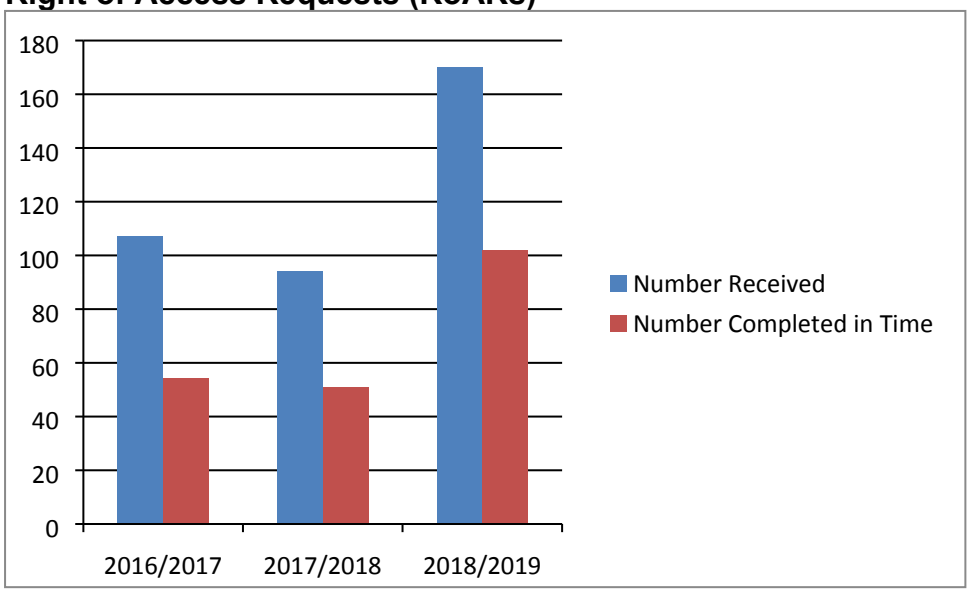
Appendix 2: FOI & RoAR Statistics

Freedom of Information (FOI) Requests



Year	Number Received	Number Completed in Time	% Completed in Time
2016/2017	1368	1058	77%
2017/2018	1378	1122	81%
2018/2019	1436	1273	89%

Right of Access Requests (RoARs)



Year	Number Received	Number Completed in Time	% Completed in Time
2016/2017	107	54	50%
2017/2018	94	51	54%
2018/2019	170	102	60%