Report of the Data Protection Officer

AUDIT COMMITTEE – 18TH APRIL 2018

GENERAL DATA PROTECTION REGULATION PROGRAMME

1. Purpose of the Report

1.1 The purpose of this report is to provide the Audit Committee with an update on the progress being made towards meeting the requirements of the General Data Protection Regulations (GDPR) that become enforceable on 25th May 2018.

2. Recommendations

2.1 It is recommended that the Audit Committee:

i. Considers the report and the progress made to date to prepare for the GDPR coming into force;

ii. Obtains assurance regarding the actions in place to address the key areas ready for the 25th May 2018;

iii. Receives further reports at subsequent meetings to provide information and assurances regarding the Authority's compliance with the GDPR.

3. Background

3.1 The GDPR are new regulations that will come into effect on the 25th May 2018, alongside a new UK Data Protection Act that will completely replace the existing Data Protection Legislation in the UK.

3.2 The GDPR enhances the current legislation and introduces new requirements that must be implemented within the Council.

3.3 Considerable work has been undertaken by the Information Governance Team over the last 18 months for what has been a significant programme of activity. In managing the programme, there have been 7 broad work streams:

- Revising processes to accommodate enhanced and two new 'Rights of Individuals' when processing and retaining their personal data.
- Reviewing and implementing revised Accountability & Governance arrangements, including the appointment of a Data Protection Officer
- Review of the Data Breach Notification process
- Transfers of Information arrangements
- Communications – internally and with third parties including Service Users.
- Review and updating of relevant IG Policies
- Preparing and delivering GDPR Training and Awareness

3.4 In addition to the above work streams, a significant and extensive requirement has been to undertake a data process mapping exercise. This is required for every process that includes the processing of personal and / or sensitive data. For each process it has been recorded; how we obtain the data; what we do with it; who we share it with – including if appropriate any sharing agreements in place; and how long we will keep it for. The output from this exercise has been issued to process owners within Business Units to inform and flag risks, so that actions can be taken to mitigate risks to the business and ensure the Council is compliant with the regulations.

3.5 To date this exercise has identified 172 individual processes and involved significant input from the IG Team to support the business units to complete this task. As of the 10th April 168 processes have been mapped in a central repository held by IG, with the remainder on schedule for completion by 30th April. This position is evolving and is expected to change on a frequent basis, as awareness of GDPR heightens and GDPR 'in force' date approaches.

3.6 Work will continue with the support of Internal Audit to ensure as many of the actions arising from the data process mapping exercises are implemented before the 25th May. This will be done on a risk basis where the nature of the data held is the greatest volume, variability and sensitivity.

3.7 The process mapping status of each Business Unit is:

- BU1 Education Early Start & Prevention - 1 outstanding
- BU2 Adult Social Care and Health– Completed
- BU3 Children's Social Care & Safeguarding - Completed
- BU4 Economic Regeneration – 1 process outstanding
- BU5 Culture, Housing & Regulation - Completed
- BU6 Environment & Transport - Completed
- BU7 Customer Services - Completed
- BU8 Stronger, Safer & Healthier Communities– Completed
- BU10 Public Health– 1 process outstanding
- BU11 Assets - Completed
- BU12 Customer, Information and Digital Services - Completed
- BU13 Finance - Completed
- BU14 Human Resources & Business Support - Completed
- BU15 Business Improvement & Communications – 1 outstanding
- BU17 Legal Services - Completed
- BU18 Health and Safety - Completed
- BU19 Governance & Member Support – Completed

Note – Business Units 9 and 16 no longer exist following recent restructures.

3.8 <u>Other Workstreams:</u>

3.8.1 <u>Rights of Individuals:</u>

Meetings have been held to agree the Council's approach to responding to requests from Data Subjects to exercise their rights. Work is progressing in Customer Services and Information Governance teams to put in place

processes to ensure BMBC can support these requests as defined under GDPR requirements and timeframes. Detailed information and request forms will be incorporated into the Council's privacy statement to be held on the internet.

3.8.2 Accountability & Governance:

A presentation was given to Executive and Service Directors on 20th March 2018 covering the Council's approach to implementing GDPR requirements.

A revised governance framework for managing and demonstrating the accountability for data protection is currently being developed building on the existing Information Governance Board, the role of the Data Protection Officer (see below), Internal Audit and the general accountability framework for all Business Unit Service Directors.

3.8.3 Communications:

Meetings have been held with Communications to discuss and agree the approach and timelines required for publication of various GDPR related information and ensuring the Council's website contains the updated privacy notices etc.

3.8.4 Policies:

Data Protection Policy – This was considered and agreed at the IG Board Meeting on 16th March 2018 following consultation with Business Units. The Policy has been drafted 'as at' 25th May when it will be formally published.

Information Security Computer Usage Policy – This Policy was also considered and agreed at the IG Board Meeting on 16th March 2018 following consultation with Business Units.

Both the above policies have received Union approval on the 28th March and have been submitted to SMT for approval.

3.8.5 Training and Awareness:

Quick reference guides have been prepared to be published on the Information Governance Intranet pages for business support and guidance.

A specific GDPR training module is currently being prepared. This will be accessed through the Council's on-line training system. All staff will be required to undertake the training and pass the on-line test – failure to complete the training or pass the on-line test within approved timelines will have result in individuals having their network access removed until this is completed.

Further training and awareness activities are being planned over the next few months. This will include training for non-network users.

3.8.6 Programme Plan:

An updated detailed Programme Plan is attached at Appendix A.

3.8.7 Data Protection Officer (DPO)

The GDPR places a statutory requirement for organisations such as local authorities to appoint a person to fulfil the role of Data Protection Officer (DPO). This role has specific responsibilities that are highlighted in Appendix B.

The DPO role is now being undertaken by the Head of Internal Audit and Corporate Anti-Fraud. Arrangements are currently being prepared to ensure the appropriate support is available including formalising reporting to the Audit Committee, Information Management Board, SMT and Cabinet.

4. List of Appendices

4.1 Appendix A – Internal Audit Plan by Directorate
Appendix B – Summary of Planned Coverage

5. Background Papers

5.1 GDPR Project working papers, reports and planning information.

Appendix A – GPDR Programme Plan

Unique Ref	DESCRIPTION / TASK	Due By	Completed
1	**GDPR process Flow Mapping**	30/04/2018	
1.1	**Ensure all Processes Mapped across BMBC - refer to mapping tracker for progress** **Ensure Processes with Schedule 3 Law Enforcement of DPB updated to reflect additional requirements.**	30/04/2018	
2	**Individuals rights**	30/04/2018	
2.1	**the right to be informed**	30/04/2018	
2.1.1	review of individuals right to take place in line with ICO code of practice	30/03/2018	17/11/2017
2.1.2	review ICO guidance and establish best practice for privacy notices.	25/07/2017	17/11/2017
2.1.3	update centrally held BMBC Privacy Notice	15/04/2018	
2.1.4	produce and issue Quick Ref Guide / minimum standards for Business use	17/11/2017	17/11/2017
	Identify which teams need to document business specific privacy notice. Ensure that this extends to include both compliance with GDPR and reference Schedule 3 law enforcement requirements under DPB. Issue Guidance / templates. Support publication from main BMBC internet site.		
2.1.5	engage with other Councils to ascertain their approach and status to Privacy Notices - share documents and inform our next steps	22/12/2017	12/01/2018
2.1.6	produce Privacy Notice Service Specific Template and Process Flow	18/01/2018	18/01/2018
2.1.7	undertake assurance activity to ensure all data privacy notices are identified, registered and meet new GDPR Legislation.	30/03/2018	
2.1.8	create central repository for Privacy Notices	28/02/2018	07/02/2018
2.1.9	work with corporate comms about wording / publishing privacy notice on internet / external	31/03/2018	
2.1.10	work with legal to review / communicate privacy statement within BMBC staff contracts	30/03/2018	
2.1.11	work with Customer Services to ensure requirements are reflected in their processes / correspondence	30/03/2018	
2.2	**The right to erasure**	30/04/2018	
2.2.1	Devise alongside the business a process to respond to requests	30/04/2018	
2.2.2	The current information flow mapping exercise will identify all legal basis for process for processing, where consent is used try to find alternative	30/04/2018	
2.2.3	Put in place technical capability of identification and erasure of all systems - ICO Recommendation	25/05/2018	

Unique Ref	DESCRIPTION / TASK	Due By	Completed
2.2.4	Produce and issue guidance notes / minimum standards for the Business to implement.	17/11/2017	17/11/2017
2.2.5	External communications - include in privacy notices	20/05/2018	
2.3	**Rights in relation to automated decision making and profiling**	30/04/2018	
2.3.1	understand the new requirements	30/03/2018	31/01/2018
2.3.2	Identify from process mapping if this applies to BMBC	30/04/2018	
2.3.3	External comms to be included in Privacy Notice	30/04/2018	
2.3.4	Devise alongside the business a process to respond to requests	30/04/2018	
2.4	**The right to Object**	30/04/2018	
2.4.1	Understand under what circumstances we need to apply	31/01/2018	31/01/2018
2.4.2	Produce and issue guidance notes / minimum standards for the Business to implement.	17/11/2017	17/11/2017
2.4.3	External comms to be included in Privacy Notice	30/04/2018	
2.4.4	Devise alongside the business a process to respond to requests	30/04/2018	
2.5	**The right to rectification**	30/04/2018	
2.5.1	Understand under what circumstances we need to apply	31/01/2018	31/01/2018
2.5.2	Produce and issue guidance notes / minimum standards for the Business to implement.	17/11/2017	17/11/2017
2.5.3	External comms to be included in Privacy Notice	30/04/2018	
2.5.4	Devise alongside the business a process to respond to requests	30/04/2018	
2.6	**The right to data portability**	30/04/2018	
2.6.1	Understand under what circumstances we need to apply	31/01/2018	31/01/2018
2.6.2	Produce and issue guidance notes / minimum standards for the Business to implement.	17/11/2017	17/11/2017
2.6.3	External comms to be included in Privacy Notice	30/04/2018	
2.6.4	Devise alongside the business a process to respond to requests	30/04/2018	
2.7	**the right to restrict processing**	30/04/2018	
2.7.1	Understand under what circumstances we need to apply	30/03/2018	31/01/2018
2.7.2	Produce and issue guidance notes / minimum standards for the Business to implement.	17/11/2017	17/11/2017
2.7.3	External comms to be included in Privacy Notice	30/04/2018	
2.7.4	Devise alongside the business a process to respond to requests	30/04/2018	

Unique Ref	DESCRIPTION / TASK	Due By	Completed
2.8	**the right of access**	30/04/2018	
2.8.1	understand the new requirements - Tthis includes GDPR / Law enforcement	30/03/2018	31/01/2018
2.8.2	revise subject access procedures and documentation provided to individuals and internet & intranet pages	30/04/2018	
2.8.3	Produce and issue guidance notes / minimum standards for the Business to implement.	17/11/2017	17/11/2017
2.8.4	External comms to be included in Privacy Notice	30/04/2018	
2.8.4	Devise alongside the business a process to respond to requests	30/04/2018	
3	**Accountability and Governance**	30/04/2018	
3.1	**Governance**		
3.1.1	Awareness of the need to address GDPR by functional Managers	25/05/2018	
3.1.2	Regular audit reports on GDPR compliance submitted to IG Board	30/04/2018	
3.2	**Security Responsibilities** : pseudonymisation and encryption system capabilities . Processes to ensure confidentiality integrity availability restore and test	30/04/2018	
3.2.1	understand the new requirements	31/01/2018	31/01/2018
3.2.2	Ensure all processes and systems are in place - Includeing Encryption Policy	30/03/2018	
3.2.3	Ensure databases encrypted within the business	30/03/2018	
3.2.4	Enusre utilise pseudonymuisation techniques when dealing with external contacts e.g NHS	30/03/2018	
3.3	**Network Security Directive**	30/03/2018	
3.3.1	understand the new requirements	31/01/2018	31/01/2018
3.3.2	Ensure all processes and systems are in place	30/03/2018	
3.3.3	Ensure regular internal network security testing	30/03/2018	
3.3.4	Implement cyber essentials plus	30/03/2018	
3.3.5	Implement PCI DSS	31/12/2018	
3.4	**Risk Management**	30/03/2018	21/03/2018
3.4.1	GDPR risk (fines and legal actions) on corporate risk register	30/03/2018	21/03/2018
3.5	**Data Protection impact Assessments**	15/05/2018	
3.5.1	Understand GDPR requirements and define our approach. Ensure all requirements of both GDPR / Schdule 3 DPB Law enforcement incorporated.	15/05/2018	
3.5.2	Engage with Project team Manager to ensure all new projects have PIA's completed and evidence retained	15/03/2018	

Unique Ref	DESCRIPTION / TASK	Due By	Completed
3.5.3	Complete DIP test of existing projects to identify gaps in process	30/03/2018	
3.5.4	Create new assessment tool / Procedures inc escalation IG . DPO IG Board	07/05/2018	
3.5.6	Design and implement a central repository for DPIA	30/04/2018	
3.5.7	Issue comms / training to internal stakeholders	15/05/2018	
4	**Legal Basis for processing**		
4.1	**Consent**	25/05/2018	
4.1.1	Review current consent models - the information flow mapping exercise will identify where processing is taking place on the basis of consent	30/04/2018	
4.1.2	Review ICO guidance and establish best practice for Consent for both adult / child. Publish quick reference guides for the business to follow.	17/11/2017	
4.1.3	Identify if any centrally held data consent information that are signposted to by the business - online processing	25/05/2018	
4.1.4	Undertake assurance activity to ensure all Consent notices meet new GDPR Legislation	25/05/2018	
4.2	**Children's personal Data**	25/05/2018	
4.2.1	the information flow mapping exercise will identify where processing is taking place on the basis of consent	30/04/2018	
4.2.2	Review ICO guidance and establish best practice for Consent for both adult / child. Publish quick reference guides for the business to follow.	17/11/2017	17/11/2017
4.2.3	Share quick reference guides with Service Director BU03	20/12/2017	20/12/2017
4.2.4	Identify if any centrally held data consent information that are signposted to by the business - online processing	25/05/2018	
4.2.5	Undertake assurance activity to ensure all Consent notices meet new GDPR Legislation	25/05/2018	
4.3	**Controllers / Processor Responsibilities**	25/05/2018	
4.3.1	Understand who are controllers / joint controllers and Processors - engage with legal as required. Use information to inform data mapping and education sessions	30/04/2018	
4.4	**Contracts**	25/05/2018	
4.4.1	Understand GDPR requirements for Contracts	30/03/2018	
4.4.2	Review / Amend Staff contracts to remove reference to processing with consent (R Winter raised issue with current contracts)	25/04/2018	
4.4.3	Support Draft contracts / agreement clauses for BMBC acting as a **processor** (can be utilised for school support services e.g. code green SIMS support) -	30/03/2018	
4.4.4	Prepare and issue agreed contract / agreement processor clauses to schools	30/03/2018	

Unique Ref	DESCRIPTION / TASK	Due By	Completed
4.4.5	Support Draft contracts / agreement clauses for BMBC acting as a **contoller**	30/03/2018	
4.4.6	Support Contracts team to implement new contract and review existing clauses for us acting as a **Controller.**	30/04/2018	
4.4.7	Support Procurement to implement new contract and review existing clauses	30/04/2018	
4.4.8	Dip test contracts to ensure GDPR requirements adhered to	25/05/2018	
4.5	**Certification - approved codes of conduct and certification mechanisms for GDPR**	25/05/2018	
4.5.1	Understand certification requirements for GDPR	25/05/2018	
4.6	**Data Protection Officer**	25/05/2018	
4.6.1	identify the requirements of the role. (existing role/new role)	17/11/2017	17/11/2017
4.6.2	Appoint individual to undertake role	25/05/2018	
4.6.3	Define roles and support for DPO	25/05/2018	
4.6.4	DPO to gain relevent qualification	28/02/2018	16/02/2018
4.6.5	Establish telephone number and email for DPO contact information	28/02/2018	28/02/2018
4.7	**Breach Notification**	30/04/2018	
4.7.1	Understand the new ICO powers (includes any breach of the new law). Include requirements under GDPR / Schedule 3 Law enforcement of DPB	30/03/2018	28/02/2018
4.7.2	Communicate with the business new requirements	30/04/2018	
4.7.3	Update BMBC training material / Policies requirements	30/04/2018	
4.8	**Section 3 - Law enforcement**	30/04/2018	
4.8.1	Understand parts of the council impacted with this part of legislation - has to be a statutory duty.	28/02/2018	
4.8.2	Understand requirements to comply in additon to GDPR	28/02/2018	
4.8.3	Communciate additional requirmenets with impacted BU's / Serivces	30/03/2018	
4.8.4	Review process mapping for effected areas to ensure meet requirements of Shcedule 3	30/04/2018	
5	**Transfers of information**	30/04/2018	
5.1	**International transfers**	30/03/2017	
5.1.1	Understand GDPR requirements for International transfers	11/10/2017	11/10/2017
5.1.2	review if any international transfers identified by the process flow mapping	30/04/2018	
5.1.3	check box included in data process flow chart re. international	11/10/2017	20/10/2017
5.1.4	Build into DPIA's to flag if subsequent processes will involve international transfers	30/04/2018	31.03.18

Unique Ref	DESCRIPTION / TASK	Due By	Completed
6	**Policies Protocols and Guidance**	25/05/2018	
6.1	**Policies Protocols and Guidance - Review of all policies with reference to data protection legislative requirements to reflect GDPR - See policy tracker for review status**	25/05/2018	
6.1.1	Data Protection Policy Include GDPR / DPB / Schedule 3 Law Enforcement	30/03/2018	16.03.18
6.1.2	Freedom on Information Policy	30/03/2018	
6.1.3	Information security and computer usage Policy	30/03/2018	16.03.18
6.1.4	Records Management Policy	30/03/2018	
6.1.5	Privacy Impact Assessments Policy	30/03/2018	
7	**Training & Awareness material**	24/05/2018	
7.1	**Training & Awareness**	24/05/2018	
7.1.1	Mandatory GDPR training course written for all staff	01/05/2018	
7.1.2	GDPR traning course completed by all colleagues	24/05/2018	
7.1.3	GDPR requirements included in staff induction training	01/05/2018	
8	**Gap Analysis**	30/04/2018	
8.1	**Gap Analysis**	25/05/2018	
8.1.1	Complete an initial gap analysis to ascertain compliance position - determine Business requirements for gap analysis	22/12/2017	22/12/2017
8.1.2	Review gap analysis to ascertain compliance	25/05/2018	
9	**Communication**		
9.1	**Communication support**	30/04/2018	
9.1.1	Identify comms support	28/02/2018	27/02/2018
9.1	**Communication Plan**	30/04/2018	

Unique Ref	DESCRIPTION / TASK	Due By	Completed
9.1.1	Devise Communication Plan: Incorporating BLT awareness - ED Poster Campaign GDPR awareness Blogging IG Corporate comms (BMBC employed staff) External stakeholders (Service users / members of public / customers Media to be used Equality and inclusion requirements met	28/02/2018	27/02/2018
9.2	IG / IS intranet site	28/02/2018	09/02/2018
9.2.1	Create and launch new intranet site with GDPR section for internal awareness	28/02/2018	09/02/2018
10	**IG Structure - Roles and Responsibilities**	25/04/2018	
10.1	**IG structure**	25/04/2018	
10.1.1	Define IG structure	25/04/2018	
10.2	**Roles and Responsibilities**	25/05/2018	
10.2.1	Produce roles and responsible matrix	30/03/2018	16/03/2018
10.2.2	Communicate with stakeholders responsibility	25/05/2018	

Appendix B Data Protection Officer – Roles and Responsibilities

The Council has an obligation as a public authority, which processes personal and special categories of data, under Data Protection Legislation to appoint a Data Protection Officer.

To fulfil their obligations of this role for the Council the appointed Data Protection Officer will:

- Be fundamental in assisting the Council demonstrate its accountability for the proper management of personal and special data;
- Have involvement in a timely manner in all issues which relate to the protection of personal and special data that we hold about individuals. This includes all data breaches reported and investigated by the Council;
- Report and have unfettered direct access to senior management in the Council on data protection matters. The independent and impartial advice and recommendations made by the DPO with regards data protection matters will be taken into consideration by senior management;
- Be consulted and advise on changes to existing and the implementation of new systems that are used for the purpose of processing personal and or special data;
- Be provided with adequate support from the Council in terms of resources, infrastructure and staff to fulfil the requirements of the role;
- Ensure there is effective monitoring in place and compliance with Data Protection laws, including the management if internal data protection activities, ensuring data processing staff are trained and commission and conduct appropriate audits;
- Have up to date knowledge of the Council's obligations regarding data protection legislation and hold a relevant qualification. This will be supported with continuous training;
- Work alongside and cooperate with the Council's supervisory authority (the Information Commissioner Officer) and serve as the contact point for the supervisory authority on issues relating to the processing of personal data;
- Be available for inquiries from data subjects and staff members on issues relating to data protection practices and the failure to comply with data protection principles; and
- Be bound by confidentiality concerning the performance of their task.

Contact details for the Councils Data Protection Officer: DPO@barnsley.gov.uk