BARNSLEY METROPOLITAN BOROUGH COUNCIL

Joint report of the IT Service Director
& Head of Internal Audit and Corporate
Anti-Fraud to the Audit Committee
to be held on the 17th January, 2018

INFORMATION COMMISSIONERS AUDIT AND GENERAL DATA PROTECTION REGULATIONS PROGRAMME

1. Purpose of the Report

The purpose of this report is to provide Audit Committee with an overview of the recent Information Commissioners Office (ICO) audit and progression towards General Data Protection Regulations (GDPR) compliance.

2. Background

The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

The ICO sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

The Council agreed to a consensual audit of its processing of personal data, observing how the Council deliver training and awareness to its employees and processing of information requests.

An introductory meeting was held on 11th August 2017 with representatives of the Council to identify and discuss the scope of the audit and subsequently to agree the schedule of interviews.

The audit field work was undertaken at Gateway Plaza and Shortwood Villas between 17th October and 19th October 2017.

3. ICO Observations and Actions

It is the Council's responsibility to meet the challenges of safeguarding the information of their service users and the outcome of this audit was an opportunity to implement new measures to ensure that the Council continue to strengthen their existing policies, procedures and practices.

The ICO made significant recognition of the strong leadership and good practice the Council have embedded. In particular, they cited the excellent online training provision, comprehensive case management system for processing Freedom of Information requests and Shortwood was identified as having very well established processes for managing paper records.

In addition, they highlighted some areas to be considered for further improvement e.g. developing a training package for non-computer users, the performance of Freedom of Information requests to be monitored and discussed during team meetings, implementing processes for deleting electronic data and introducing KPI's for records management with representation on the Information Governance Board.

The Executive Summary can be viewed here: https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/barnsley-metropolitan-borough-council/

The ICO have highlighted many of our key strengths and indeed suggested a number of urgent and more challenging areas for improvement, for example:

- To continue with our transition to SharePoint;
- To ensure the retention and disposal of records complies with our policies;
- To ensure that all confidential waste bins are secure;
- To develop and monitor a number of new Corporate performance indicators for records management; and
- To implement the monitoring and compliance of records management across the Council.

The overall audit opinion for the Council is 'Reasonable assurance':

> *There is a reasonable level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA.*
>
> *The ICO have made a limited assurance assessment in respect of Records Management, and two reasonable assurance assessments, in respect of Training and Awareness and Freedom of Information, where controls could be enhanced to address the issues which are presented fully in the separate 'action plan', along with management responses.*

There are a number of recommendations for the Council to act on but to put these into perspective the majority are medium or low priority – which is great news!

An action plan has been developed by the Council and will be facilitated by Internal Audit; the Information Governance Board and Audit Committee will continue to receive regular reviews of progress to date.

The ICO will contact the Council during September 2018 to request an updated Action Plan, in order to carry out a follow up audit, this will be a desk based review using the updated action plan and any supporting evidence the Council supplies.

4. GDPR

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

GDPR enhances existing legislation and also introduces some new requirements that must be implemented within the Council.

The project has identified 7 work streams:

- Individuals Rights
- Accountability & Governance
- Breach Notification
- Transfers of Information
- Communications
- Policies
- Training and Awareness

In addition to the above work streams, a significant and extensive new requirement is that the Council undertakes a process mapping exercise.

This is required for every process that includes the processing of personal and / or sensitive data. This process will record; how we obtain the data; what we will do with it; who we will share it with – including if appropriate sharing agreements in place; and how long we will keep it for.
The output from this exercise will be issued to process owners to inform and flag risks, so that actions can be taken to mitigate risks to the business and ensure the Council is compliant with this regulation.

During this period significant resource has been given to supporting the business units to complete this task. It has however been recognised, due to the volume of processes and gaps identified, that there is a requirement to adjust the initial internally set milestone of the 31/12/17 to the 31/03/18. This will be monitored on a regular basis by the Information Governance Team to ensure progress continues to meet timelines; and that this along with other supporting GDPR requirements are completed in readiness for GDPR coming into effect on the 25th May 2018.

There are a total of 78 processes mapped in the 'live' system.

The following business units have completed their process flow maps:

- BU12 Information Technology Service
- BU13 Finance
- BU17 Legal Services (NEW)
- BU19 Governance & Member Support

Work has commenced in the following business units, with additional meetings scheduled in the diary to fully complete the process mapping exercise (based on current business unit process information provided to date):

- BU1 Education Early Start & Prevention
- BU2 Adult Social Care and Health
- BU3 Children's Social Care & Safeguarding
- BU7 Customer Services
- BU8 Stronger, Safer & Healthier Communities
- BU11 Assets
- BU15 Business Improvement & Communications
- BU18 Health & Safety

Gaps have been identified in the following business units where engagement is required during the next period to schedule meetings and complete the process mapping exercise:

- BU4 Economic Regeneration - Majority complete, one new area outstanding
- BU5 Culture, Housing & Regulation - 3 areas complete, 3 areas outstanding.
- BU6 Environment & Transport – Whole business unit outstanding
- BU10 Public Health – Initial meetings held, overlaps to be identified, meetings to be scheduled & processes to be mapped
- BU14 Human Resources & Business Support – Two processes mapped for HR, Business support to be completed.

Other Work streams:

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

Accountability & Governance:

With regards appointing a Data Protection Officer (DPO), a paper was submitted to Information Governance Board for approval on 16/11/2017 assigning the Head of Internal Audit the role of DPO.

Training and Awareness:

Information sharing training day held 25/10/2017 with representatives across the business attending. The training covered Information Sharing Protocols and Agreements, Purpose and Legal basis, Caldicott 2 & 3, Data transfers between organisations, Digital Economy Act and GDPR.

Programme Plan:

Appendix A.

APPENDIX A – GDPR PROGRAMME PLAN

UNIQUE REF	DESCRIPTION / TASK	DUE BY	COMPLETED
1	**GDPR process Flow Mapping**	**Fri 30/03/18**	
1.1	**Ensure all Processes Mapped across BMBC - refer to mapping tracker for progress**	**Fri 30/03/18**	
2	**Individuals rights**	**Fri 30/03/18**	
2.1	**The right to be informed**	**Fri 30/03/18**	
2.1.1	review to take place in line with ICO code of practice	Fri 30/03/18	17/11/2017
2.1.2	Review ICO guidance and establish best practice for privacy notices.	Tue 25/07/17	17/11/2017
2.1.3	Identify and update any centrally held data privacy notices by BMBC that are signposted to by the business.	Fri 31/01/18	
2.1.4	Engage with other Councils to ascertain their approach and status to Privacy Notices - share documents and inform our next steps	Fri 22/12/17	Fri 22/12/17
2.1.5	Produce and issue guidance notes / minimum standards for the Business to implement.	Thu 17/11/17	17/11/2017
2.1.6	Undertake assurance activity to ensure all data privacy notices meet new GDPR Legislation.	Fri 30/03/18	
2.1.7	Work with corporate comms about wording / publishing privacy notice on internet / External	Fri 31/01/18	
2.1.8	Work with Claire Dobbie Customer Services to ensure requirements reflected in SAR correspondence	Fri 31/01/18	
2.2	**The right to erasure**	**Fri 30/03/18**	
2.2.1	Devise alongside the business a process to respond to requests	Fri 30/03/18	
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	Fri 30/03/18	
2.2.3	Put in place technical capability of identification and erasure of all systems - ICO Recommendation	Fri 31/01/18	
2.2.4	Produce and issue guidance notes / minimum standards for the Business to implement.	Thu 17/11/17	17/11/2017
2.2.5	External communications - include in privacy notices	Fri 31/01/18	
2.3	**Rights in relation to automated decision making and profiling**	**Fri 30/03/18**	
2.3.1	understand the new requirements	Fri 30/03/18	
2.3.2	Identify from process mapping if this applies to BMBC	Fri 30/03/18	
2.3.3	External comms to be included in Privacy Notice	Fri 30/03/18	
2.3.4	Devise alongside the business a process to respond to requests	Fri 30/03/18	
2.4	**The right to Object**	**Wed 26/01/18**	
2.4.1	Understand under what circumstances we need to apply	Fri 31/01/18	
2.4.2	Produce and issue guidance notes / minimum standards for the Business to implement.	Thu 17/11/17	17/11/2017

UNIQUE REF	DESCRIPTION / TASK	DUE BY	COMPLETED
2.4.3	External comms to be included in Privacy Notice	Fri 30/03/18	
2.4.4	Devise alongside the business a process to respond to requests	Fri 30/03/18	
2.5	**The right to rectification**	**Wed 26/01/18**	
2.5.1	Understand under what circumstances we need to apply	Fri 31/01/18	
2.5.2	Produce and issue guidance notes / minimum standards for the Business to implement.	Thu 17/11/17	17/11/2017
2.5.3	External comms to be included in Privacy Notice	Fri 30/03/18	
2.5.4	Devise alongside the business a process to respond to requests	Fri 30/03/18	
2.6	**The right to data portability**	**Wed 26/01/18**	
2.6.1	Understand under what circumstances we need to apply	Fri 31/01/18	
2.6.2	Produce and issue guidance notes / minimum standards for the Business to implement.	Thu 17/11/17	17/11/2017
2.6.3	External comms to be included in Privacy Notice	Fri 30/03/18	
2.6.4	Devise alongside the business a process to respond to requests	Fri 30/03/18	
2.7	**the right to restrict processing**	**Fri 30/03/18**	
2.7.1	Understand under what circumstances we need to apply	Fri 30/03/18	
2.7.2	Produce and issue guidance notes / minimum standards for the Business to implement.	Thu 17/11/17	17/11/2017
2.7.3	External comms to be included in Privacy Notice	Fri 30/03/18	
2.7.4	Devise alongside the business a process to respond to requests	Fri 30/03/18	
2.8	**the right of access**	**Fri 30/03/18**	
2.8.1	understand the new requirements	Fri 30/03/18	
2.8.2	revise subject access procedures and documentation provided to individuals and internet & intranet pages	Fri 30/03/18	
2.8.3	Produce and issue guidance notes / minimum standards for the Business to implement.	Thu 17/11/17	17/11/2017
2.8.4	External comms to be included in Privacy Notice	Fri 30/03/18	
2.8.4	Devise alongside the business a process to respond to requests	Fri 30/03/18	
3	**Accountability and Governance**	**Fri 30/03/18**	
3.1	**Security Responsibilities: pseudonymisation and encryption system capabilities. Processes to ensure confidentiality integrity availability restore and test**	**Fri 30/03/18**	
3.1.1	understand the new requirements	Fri 31/01/18	
3.1.2	Ensure all processes and systems are in place	Fri 30/03/18	
3.2	**Network Security Directive**	**Wed 11/01/18**	
3.2.1	understand the new requirements	Fri 31/01/18	

UNIQUE REF	DESCRIPTION / TASK	DUE BY	COMPLETED
3.2.2	Ensure all processes and systems are in place	Fri 30/03/18	
3.3	**Data Protection impact Assessments**	**Fri 30/03/18**	
3.3.1	Understand GDPR requirements	Fri 30/03/18	
3.3.2	Engage with Project team Manager to ensure all new projects have PIA's completed and evidence retained	Fri 30/03/18	
3.3.3	Complete DIP test of existing projects to identify gaps in process	Fri 30/03/18	
3.3.4	Create new assessment tool / Procedures inc escalation IG. DPO IG Board	Fri 30/03/18	
3.3.5	Design and implement a central repository for DPIA	Fri 30/03/18	
3.3.6	Issue comms to internal stakeholders	Fri 30/03/18	
4	**Legal Basis for processing**		
4.1	**Consent**		
4.1.1	Review current consent models - the information flow mapping exercise will identify where processing is taking place on the basis of consent	Fri 30/03/18	
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.	Thu 17/11/17	17/11/2017
4.1.3	Identify if any centrally held data consent information that are signposted to by the business - online processing	Fri 30/03/18	
4.1.4	Undertake assurance activity to ensure all Consent notices meet new GDPR Legislation	Fri 30/03/18	
4.2	**Children's personal Data**	**Wed 26/01/18**	
4.2.1	the information flow mapping exercise will identify where processing is taking place on the basis of consent	Fri 30/03/18	
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.	Thu 17/11/17	17/11/2017
4.2.3	Share quick reference guides with Service Director BU03	Wed 20/12/17	Wed 20/12/17
4.2.4	Identify if any centrally held data consent information that are signposted to by the business - online processing	Fri 30/03/18	
4.2.5	Undertake assurance activity to ensure all Consent notices meet new GDPR Legislation	Fri 30/03/18	
4.3	**Controllers / Processor Responsibilities**	**Wed 20/12/17**	
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	Wed 20/02/17	
4.4	**Contracts**	**Fri 30/03/18**	
4.4.1	Understand GDPR requirements for Contracts	Fri 30/03/18	

UNIQUE REF	DESCRIPTION / TASK	DUE BY	COMPLETED
4.4.2	Review / Amend Staff contracts to remove reference to processing with consent (R Winter raised issue with current contracts)		
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) -	Fri 31/01/18	
4.4.4	Prepare and issue agreed contract / agreement processor clauses to schools	Fri 28/02/18	
4.4.5	Support Draft contracts / agreement clauses for BMBC acting as a **controller**	Fri 31/01/18	
4.4.6	Support Contracts team to implement new contract and review existing clauses for us acting as a **Controller.**	Fri 30/03/18	
4.4.7	Support Procurement to implement new contract and review existing clauses	Fri 30/03/18	
4.4.8	Dip test contracts to ensure GDPR requirements adhered to	Fri 30/03/18	
4.5	**Certification - approved codes of conduct and certification mechanisms for GDPR**	**Fri 30/03/18**	
4.5.1	Understand certification requirements for GDPR	Fri 30/03/18	
4.6	**Data Protection Officer**	**Fri 30/01/18**	
4.6.1	identify the requirements of the role. (existing role/new role)	Wed 11/10/17	17/11/2017
4.6.2	Appoint individual to undertake role	Fri 30/01/18	
4.7	**Breach Notification**	**Wed 11/03/17**	
4.7.1	Understand the new ICO powers (includes any breach of the new law)	Wed 11/03/17	
4.7.2	Communicate with the business new requirements	Fri 30/03/18	
4.7.3	Update BMBC training material / Policies requirements	Fri 30/03/18	
5	**Transfers of information**	**Fri 30/03/18**	
5.1	**International transfers**	**Wed 11/03/17**	
5.1.1	Understand GDPR requirements for International transfers		
5.1.2	review if any international transfers identified by the process flow mapping	Wed 11/03/17	
5.1.3	check box included in data process flow chart re. international	Wed 11/10/17	20/10/2017
5.1.4	Build into DPIA's to flag if subsequent processes will involve international transfers	Fri 30/03/18	
6	**Policies Protocols and Guidance**	**Fri 30/03/18**	
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**	**Fri 30/03/18**	
6.1.1	Information Governance Policy	Fri 30/03/18	
6.1.2	Data Protection Policy	Fri 30/03/18	
6.1.3	Freedom on Information Policy	Fri 30/03/18	

UNIQUE REF	DESCRIPTION / TASK	DUE BY	COMPLETED
6.1.4	Information security and computer usage Policy	Fri 30/03/18	
6.1.5	Records Management Policy	Fri 30/03/18	
6.1.6	Privacy Impact Assessments Policy	Fri 30/03/18	
7	**Training & Awareness**	**Fri 28/02/18**	
7.1	**Training & Awareness material updated**	**Fri 28/02/18**	
8	**Gap Analysis**	**Fri 30/04/18**	
8.1	**Gap Analysis**		
8.1.1	Complete an initial gap analysis to ascertain compliance position - determine Business requirements for gap analysis	Fri 22/12/17	Fri 22/12/17
8.1.2	Review gap analysis to ascertain compliance	Fri 28/02/18	