Report of the Data Protection Officer

AUDIT COMMITTEE – 22nd July 2019

Data Protection Officer's Annual Assurance Report

1. Purpose of the Report

1.1 This report provides the Committee with the Data Protection Officer's (DPO) assessment of compliance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA2018) based on specific assurance work undertaken over the last few months and general activity during the last year.

1.2 The Council's Information Goverance Board, chaired by the Senior Information Risk Owner, the Executive Dorector, Core Services, received and considered a report from the DPO at its meeting on the 26th June. This report to the Audit Committee reflects the discussions and outcomes from the IG Board.

1.3 This report covers:

- an overview of the 12 months following the formal implementation of GDPR and the DPA 2018;
- DPO activity during the year;
- Specific assurance work undertaken and the results thereof;
- Suggested audit / assurance activity for 2019/20 and beyond;
- How the responsibilities of the DPO have been discharged;
- The response from the IG Board.

2. Recommendations

2.1 It is recommended that the Audit Committee:

i. Considers the report and notes the actions agreed to address the points raised;

ii. Specifically considers and notes the response from the IG Board;

iii. Notes the programme of assurance activity proposed and endorse that full and unfettered access is given to the DPO and/or Internal Audit staff undertaking work on his behalf to information, systems, offices and staff;

iv. Receives a 6-monthly report on progress and the results of assurance work regarding the Authority's compliance with the GDPR / Data Protection Act;

v. Be satisfied that the key responsibilities of the DPO have been discharged;

3. Overview of the last 12 months

3.1 Despite some national and local anxiety about what the day after 'GDPR-day' would bring, it passed without incident; there was no tidal wave of public interest to find out what data was being held about them. There was some national press coverage focussed largely on the new rights we all have as private citizens and of course publicity around the issues that Facebook and other large companies had regarding the use of personal data. The profile of data protection through the national press was raised but relatively briefly.

3.2 What GDPR did result in though was a renewed focus on our individual and collective responsibilities for protecting and managing the data we hold as a Council. This responsibility has been with us since the Data Protection Act 1998 of course, and whilst the GDPR and DPA2018 brought in new aspects to this arena, they haven't changed things that much in practical terms. Perhaps the most significant and beneficial, change the GDPR has brought about however are the 6 Data Protection Principles and the duty of being required to demonstrate accountability, known as the 7th Principle. I think these are pretty well understood but as a reminder, the data protection principles are:

Principle 1: lawfulness, fairness and transparency

This means that the Council will tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be processed for one of the purposes specified in the legislation (lawfulness).

Principle 2: Purpose Limitation

This means that the Council will specify what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation

This means that the Council will not store or process any personal information beyond what is strictly required.

Principle 4: Data Accuracy

This means that the Council will have in place processes for identifying and addressing out-of-date, incorrect and redundant personal information.

Principle 5: Storage Limitation

This means that the Council will, wherever possible, store personal data in a way that limits or prevents identification of the data subject and only retain it for a reasonable period, i.e. not for any longer than is appropriate.

Principle 6: Integrity and Confidentiality

This means that the Council will use appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal information is maintained at all times.

Principle '7': Accountability

This means that the Council will demonstrate that the six Data Protection Principles (outlined above) are met for all personal data for which it is responsible.

3.4 These Principles have formed the basis and backcloth to the training and guidance provided on the GDPR.

3.5 Given the activity in the run-up to the 25th May 2018 and in the 12 months afterwards, it highlighted that, like many organisations I suspect, there were aspects of data protection practice that needed review and improvement.

3.6 Although with a degree of healthy panic at times, as a Council, overall, we responded well with huge amounts of preparatory work undertaken supported by good communications and very good guidance and training. The efforts of the Information Governance Team in the preparatory work and since should be commended, in making a significant contribution to the position the Council is in.

3.7 My appointment as DPO in January 2018 also gave focus, not least to me personally but also to the 'discipline' of data protection, recognising it as a specialist area and one that carries significant responsibilities and consequences if not managed appropriately. Through the 6 Principles, the GDPR has given a structure to how we now go about good data protection practice.

3.8 Significant preparatory work was undertaken despite the fact that the Information Commissioner's Office was late in providing guidance in many practical aspects and so we did our best; and that best has been good. The key areas of work have been:

- ✓ Process mapping exercises – 180 in total across virtually every aspect of Council activity over a period of almost 2 years
- ✓ Policy review – significant reviews of key policies
- ✓ Procedure reviews for records management, subject access requests, DPIAs etc.
- ✓ Preparation of guidance – 'quick guides' as well as intranet based guidance
- ✓ POD based training involving almost 3,000 employees completing mandatory training plus face-to-face and team training sessions
- ✓ Regular communications through Straight Talk and 'Mrs. D's blog'!

3.9 In summary, I regard the Council's approach to have been robust and pretty comprehensive. What is important though is that where gaps remain and

further work identified that there is a renewed momentum and focus to properly embed good data protection practice in all aspects of the Council.

4. The Data Protection Officer (DPO)

4.1 It has been a year of development and learning. The support and assistance from the IG Team has been invaluable as part of that. Their individual and collective enthusiasm and professionalism has been outstanding.

4.2 What has also been important is to establish the DPO position within the Council. Whilst this is still 'work in progress' to some extent, what has emerged is a specific independent assurance and advisory role and a role in the day to day governance of data protection. The legislation and supporting guidance makes it clear that the role is not one of managing the IG function nor to determine policy, but to independently and objectively provide assurance. In summary, the role of the DPO is to:

- monitor internal compliance with data protection legislation
- to inform and advise on data protection obligations
- to advise on and review Data Protection Impact Assessments (DPIAs)
- to provide risk based advice where necessary
- to raise awareness of data protection issues
- to undertake and commission audits
- to be a contact point for "data subjects" (whether that be the public or internal employees)
- to be the point of contact for the Information Commissioners Office (ICO)

In fulfilling that role, a DPO must:

- act independently (which is why it can't be someone in the IG Team)
- be an expert in data protection
- be adequately resourced to carry out the role
- report into the highest management level

4.3 Later in this report I highlight how the DPO role has been discharged, again, an important element of the 7th Principle.

4.4 In terms of practical activity, over the last 18 months or so I have been involved the following:

- Undertaken accredited GDPR Foundation and Practitioner courses including sitting (and passing) exams
- input to the development of corporate training
- advice on policy review
- reviewing DPIAs and signing them off
- receiving notifications of data breaches, advising and overseeing investigations and adjudicating upon any reporting to the ICO
- ICO liaison and correspondence with complainants
- Providing ad hoc guidance, support, challenge and input to new issues
- 'Project' input for example into new Personnel files solution and attending the Digital Leadership Team in my DPO capacity

- Reporting to the IG Board and Audit Committee
- Developing and undertaking a programme of independent assurance work

4.5 There has not been any practical guidance in relation to 'how' a DPO discharges their responsibilities and so I have adopted an approach akin to my Head of Internal Audit role. There are key and very important similarities in the traits and responsibilities of both positions but they are separate.

5. Assurance Work

5.1 In fulfilment of the DPO role and to provide the Council with assurances regarding GDPR compliance, it has been necessary to develop a programme of reviews. These have been prioritised based on risk and the ease to which they could be undertaken in this first period of reflection. As the Committee is aware from previous update reports, I have delayed this assurance work to enable as much 'implementation' as possible.

5.2 These assurance reviews have not been audits as such but aimed to present to management and the IG Board my findings and to prompt management actions being identified or further work commissioned that leads to positive assurance and confidence that the Council has adequate arrangements in place to ensure high levels of compliance and minimise any risks of non-compliance and the subsequent consequences on both data subjects and the Council.

5.2 To date and forming the basis of my assurance, is the programme of work that has been undertaken across a number of areas. These assurance reviews have aimed to present to the IG Board the extent to which I can give assurances regarding compliance etc. My overall view on the Council's compliance with GDPR is also informed from the input and involvement I have had in other aspects of data protection. These are summarised later.

5.3 To date the outcome from the completed assurance reviews can be summarised in the following table:

Assurance work	Assurance Opinion	Implication of Findings		
		Low	Medium	High
Data Minimisation / Pseudonymisation	*Reasonable*	3		
Website Review	*Reasonable*	2	1	
Incident Management	*Reasonable*	1	1	
Unannounced Visits / Staff Data Survey	*Reasonable*	3	4	
Phase 1 - Process Mapping Compliance	*Limited*			1
SARS and CFIT	*Reasonable*	3	4	
Cybersecurity	*Reasonable*	3	6	1
	Total	15	16	2

5.4 Appendix A highlights the key issues arising from each assurance review showing both the positive areas as well as those where improvement in compliance or the underlying control and governance framework is required. As mentioned before, overall, my review work shows good compliance but equally an acceptance that further work is needed in a number of areas.

5.5 It should be noted that in all instances a management action has been agreed to address the implications arising from the findings in each review. As an overall response, the IG Board will ensure that management actions are being implemented within the timescales set by receiving monitoring reports during the year.

5.6 Over and above the specific assurance reviews undertaken, I have been involved in and had input into a number of other aspects of data protection and the required response to the new Regulations and Act. Such involvement and input enriches my opinion and key messages to the IG Board and Audit Committee.

5.7 Of particular significance are the following areas, both positive and where improvement or progress is required.

SharePoint - Discussions with the SharePoint systems administrator have highlighted work required around 'site owners' and to improve general compliance with the corporate file plan and operational protocols.

CCTV – It has been acknowledged that work is required to identify and capture all the installations and uses of CCTV across the Council and its maintained schools in order to provide assurances regarding compliance with the Protection of Freedoms Act, the CCTV Code of Practice and be in a position to complete a survey expected from the Surveillance Camera Commissioner later in the year.

Personnel files – This is another area where it has been acknowledged that work was needed to ensure the more efficient management of personnel records. A new SharePoint based system has been developed which will provide a practical solution to the management of various personnel records moving forwards. This has yet to go live and must be supported by clear guidance, training and on-going monitoring. A number of HR policies also need to be reviewed to support the new system.

Physical secure storage – Whilst there is generally good practice in the physical storage and security of documentation, there remains limitations in certain office areas. Although within relatively secure 'staff only' buildings, risks remain. It is accepted that there is no easy solution to this issue but one that needs to be raised to obtain the IG Board's acceptance of this risk.

Broader corporate IG capacity – I have referred earlier to the sterling work the IG Team have undertaken and continue to undertake within a very small Team. As such, any absences would significantly impact upon their capacity to provide support in this critical area of governance. The resources of the IG

Team need to be kept under review to ensure continuity, expertise and capacity.

Contracts and Law Enforcement – The GDPR and DPA2018 introduced the requirement to change standard contract provisions, data controller / processor agreements and to ensure procedures are in place to meet the Law Enforcement provisions. This work remains in progress. The IG Board need to re-assess the resources and priority given to this work to ensure it is concluded appropriately as soon as possible.

5.8 As can be seen from the specific assurance reviews and the issues in the section above, there remains work to do to further improve compliance with the GDPR and DPA2018 and generally embed good data protection practice throughout the Council.

5.9 It should be recognised however that through the assurance work and other DPO activity that there are many areas of excellent practice and obviously high levels of awareness and diligence.

5.10 In summary and to provide the IG Board and Audit Committee with an overall assurance opinion, I would assess the Council's position regarding overall compliance and having reliable and embedded good practice in place as 'reasonable', and as a simple score, a '7 out of 10'.

6. Proposed Assurance and Audit Activity

6.1 To adequately discharge my DPO responsibilities, and as set out in the Regulations and guidance, I can undertake and commission 'audits' to test compliance. The assurance reviews undertaken to date have sought to test compliance and provide the IG Board with assurances and highlight where there are opportunities to improve the control and governance of data protection.

6.2 Moving forward I shall still undertake certain reviews as I deem appropriate in my independent role. However, the IG Board and management in certain areas also need to consult with Internal Audit, through the Audit Manager, to agree specific internal audit activity. This will naturally be informed from a combination of my DPO assurance reviews and the management actions proposed and undertaken, commissions from the Board to obtain more detailed compliance assurances and requests from management as part of the normal Internal Audit planning process. All review or audit activity should be on a risk basis.

6.3 Based upon the first series of reviews and considering other areas for DPO and/or Internal Audit activity, I include in Appendix B a possible programme of work, with suggested frequencies to assist in the future planning of review resources. As mentioned above, the individual pieces of review work will need to be individually risk assessed and scoped.

6.4 The suggested programme has been formatted in a way to demonstrate indicatively which of the GDPR Principles the review activity would provide assurance on (Appendix B).

7. Discharging the responsibilities of the DPO

7.1 An important element of an organisation that has formally appointed a DPO is to be able to demonstrate how that role has been discharged as a fundamental contribution to demonstrating 'accountability' – the 7th Principle.

7.2 Attached (Appendix C) is a document developed to demonstrate how I discharge my DPO responsibilities. As can be seen the vast majority have been discharged or arrangements are in place to ensure they are as and when particular circumstances arise. Akin to other aspects of GDPR there are a few areas that require further work or consideration.

7.3 The key areas requiring further review are:

- Reviewing arrangements for reporting directly to the Chief Executive and SMT
- Reviewing arrangements for a PDR in the context of my DPO responsibilities and agree any training and development requirements
- Review arrangements for a 'deputy' DPO in circumstances where I am not available.

7.4 I will include progress on these matters in future reports to the IG Board and Audit Committee.

8. Information Governance Board – 26th June 2019

8.1 The IG Board received this DPO Annual Assurance Report at its meeting on 26th June. For the Committee's information and assurance the IG Board accepted the report and in so doing committed to the following actions:

- ✓ Reviewing the options for improving the physical storage within Westgate
- ✓ Ensure management fully implement the actions identified within the individual assurance reviews
- ✓ Consider the areas highlighted to further enhance the role of the DPO
- ✓ Ensure SMT receive the DPO Annual Assurance Report

8.2 The IG Board will receive periodic progress reports reflecting further DPO assurance activity.

9. List of Appendices

9.1 Appendix A – Key issues arising from assurance work
Appendix B – Possible Assurance and Audit Programme
Appendix C – Data Protection Officer – How Role is discharged

Contact Officer: Rob Winter, Data Protection Officer
Email: DPO@barnsley.gov.uk

Appendix A

Key issues arising from assurance work

Assurance work	Positive Key Issues and Points	Key Issues and Points for action
Data Minimisation / Pseudonymisation	✓ Encryption widely used and pseudonymisation / anonymisation used in parts of the Authority. ✓ Data breach process effective. ✓ Pseudonymisation mentioned in the mandatory GDPR eLearning. ✓ Online help available on encrypted emails. ✓ Video guide to revoking access. ✓ Quick Reference Guides for sending emails and pseudonymisation available on Intranet.	× Egress / Encryption required higher profile. × Incident reports to consider more analysis of causes / lessons learned.
Website Review	✓ BMBC website contains Privacy information that is accessible, concise and transparent. ✓ Privacy Notices recent, simple, clear and informative. ✓ Phone automated message informs caller that the call may be recorded and that data will only be processed and shared where there is a legal basis to do so.	× A few broken / outdated links found. × Privacy Notices on website still in 'template / draft' version. × Online forms did not contain sufficient GDPR information.
Incident Management	✓ Incident management policy exists and provides a framework for reporting and managing information security incidents. ✓ Sample incidents tested were promptly reported to IG. ✓ IG responded to reported incidents promptly and appropriately. ✓ Initial Impact assessments were completed within the policy timescales (24 hours). ✓ IG completed severity assessments promptly and took appropriate action.	× Some delays in incident investigations and incident closure on the part of Services. × Recommendations and deadlines not escalated to SMT when not implemented / met by the Services.
Unannounced Visits / Staff Survey	✓ Access control to buildings reasonably robust with various badge / fob controlled access and barrier controls. ✓ No personal data was visible on or around the photocopiers and they were 'signed out'. ✓ Desks were reasonably clear of sensitive data in most areas. ✓ Shredders were observed and no personal data items were left by them for shredding.	× Personal information found in recycling bins at LIFT and town centre offices. × A few unlocked screens were observed. × Lack of data minimisation and floorplate storage issues. × Iron Mountain boxes contained

Assurance work	Positive Key Issues and Points	Key Issues and Points for action
	✓ Nothing containing personal data was observed in outdoor bins. ✓ 100% of staff felt that they were 'very' or 'reasonably' aware of the GDPR and most (98%) felt that data was managed appropriately in BMBC. ✓ All surveyed staff had completed the online data training and 100% felt that this supported them in understanding how to use data in accordance with the law and BMBC policies. ✓ 98% of staff felt that the training, guidance and processes used in their role made it easy to handle data appropriately. ✓ All staff knew what constituted a data breach and most staff (95%) were aware that ICO fines for serious breaches were substantial. ✓ Most (85%) staff knew how to send a secure email. ✓ Comments around the data protection training provided to staff were positive.	personal information on the shipping label. × Survey highlighted that some staff felt systems access was more than they required. × CCTV signs were not present at one of the visited sites. × 73% of staff did not know who the DPO was.
Phase 1 Process Mapping Compliance	✓ Processes were mapped, risks identified and actions recommended to Services by the Information Governance Team. ✓ The knowledge and face to face time spent by the Information Governance Team with Services allowed the effective transfer of information. ✓ The process mapping exercise identified risks outstanding. ✓ The IG Team and DPO reflected on phase 1 and considered lessons learned in an extended IG Team meeting. ✓ From the 11 Management Actions tested, 10 were evidenced as completed and 1 had an action plan in place.	× Limiting factors and challenges to the project meant that the DPO could not provide full assurance that all risks were mitigated.
SARS and CFIT	✓ Staff can recognise a SAR and understand when the right of access applies. ✓ Staff understand what needs to be considered if a request includes information about others and there is redaction guidance. ✓ Guidance is available to staff on the management of information requests in the Management of Information Requests Procedure. This document also provides an expected timeline. ✓ There is specific guidance for Children's Social Care & Safeguarding. ✓ There is guidance to establish whether Information requests received directly by services are 'business as usual' requests or meet the criteria to	× Update of the operational procedures and associated working papers required. × Refusals, verbal requests, disclosures to children and exemptions require update. × The DPO had not been informed fully of all ICO contacts.

Assurance work	Positive Key Issues and Points	Key Issues and Points for action
	be referred to CFIT as a SAR. ✓ Procedures include the key roles and responsibilities in the handling of information requests (CFIT, Allocated Officers and IG Team). ✓ The authority's Privacy Notice is sent to customers when their request is acknowledged. ✓ BMBC have webpages 'What we do with your personal information' and 'Your Privacy' providing information to customers about their rights of access. ✓ There was an improvement between Q3 and Q4 2018/19 in terms of responding to SARS in given timescales. ✓ The council has a redaction guidance document which can be referred to in the undertaking of releasing information in connection with an information request.	
Cybersecurity Risks	✓ A number of independent assessments and reviews undertaken around cybersecurity prompting a tracking spreadsheet for Medium and High risks and fortnightly meetings with the Infrastructure Team. ✓ Achieving Cyber Essentials+ accreditation ✓ Meeting requirements of PCN standards ✓ Rigid controls in place around access controls. ✓ Policies in place for systems access. ✓ A Major Incident Response Plan has been written and a review meeting has been arranged in relation to the recent DDOS website attack. Lessons learned/recommendations will be considered and agreed and ownership will be taken by the ICT Security Lead. ✓ There is a system in place for reporting and addressing Cyber breaches and incidents. ✓ Cybersecurity contracts are regularly reviewed.	× IG Board not sufficiently informed of cybersecurity issues. × No member representative for cybersecurity as recommended in LGA assessment. × No cybersecurity specific risk register. × No specific Corporate IT Security / Cyber Resilience Strategy. × ICT Access Controls require review. × Need to formalise Cybersecurity investment planning. × Major incident reporting to be reviewed. × Revised IT HUB incident reporting arrangements needed. × Cybersecurity contract arrangements require regular review. × Cybersecurity training and policies and procedures require review.

Appendix B

Possible Audit and Assurance Programme

Updated: 21/06/2019

		Lawfulness	Purpose	Data Minimisation	Accuracy	Retention and Storage	Security	Accountability		Overseas Transfer		Suggested Frequency
GDPR		Principle (a) – lawfulness, fairness and transparency	Principle (b) – purpose limitation	Principle (c) – data minimisation	Principle (d) – accuracy	Principle (e) – storage limitation	Principle (f) – integrity and confidentiality	Accountability principle		No principle – separate provisions in Chapter V		
Data Minimisation_Pseudonymisation	Review of data minimisation and pseudonymisation. Samples to be tested for suitability of minimisation tool used.			X								Annually
Website Review	Review of outside facing authority website and the data protection perceptions of the service users. Accessibility, usability, consistency.	X						X				Annually
Incident Management	Review of the incident management process. Reporting, investigation, follow up, corporate learning etc.			X			X	X				Annually
Unannounced Visits IG_DP	Unannounced audit visits to business units and buildings to carry out review on physical controls, access and management controls.			X		X	X					Annually - different sites
Survey (GDPR)	Complete a short questionnaire to evaluate the awareness and embeddedness of GDPR/Data protection principles. 40 Staff surveyed across the Authority.							X				Annual survey to review changes year on year
Phase 1 Process Map Compliance Audit	Review of the management actions from the IG process mapping exercise. Risks, follow ups.	X	X	X	X	X	X					One off
Cybersecurity Risks	Cloud abuse, Malware, hacking, passwords, Insider threat						X					Annually
SARS and CFIT Review	Review of the SAR process and how requests are processed through CFIT.	X						X				Biennially
Accessing data from EEA under no deal Brexit	Consideration/risk assessment of third parties data transfers and identifying where these third parties are located and where data is located. Consideration of the data implications of a No Deal Brexit. Consideration of Standard Contractual Clauses (SCCs).									X		One off
Review of the Information Governance Board	Review of the effectiveness, Terms of Reference, membership, actions and progress of the IG Board							X				Triennial
SharePoint and Digital First	Permissions and access review. Cross cutting issues with Staff Data Survey, Cybersecurity reviews.			X		X						As part of project
CCTV Review	Protection of Freedoms Act 2012 (PoFA) Surveillance Camera Code of Practice (SC Code)	X				X	X	X				Biennially
Policy Review	Consideration of DP/GDPR	X										Annually
Records Management Review	Review of effectiveness and data security arrangements of the Iron Mountain records management system. Compliance, impact and VFM.			X		X	X					Biennially
Phase 2 Process Map Compliance Audit	Process, progress for the 2nd phase of the process mapping exercises.	X	X	X	X	X	X					One off
Contracts	Progress, monitoring arrangements, overall governance, register/list of contracts.	X										Biennially
Law Enforcement	Actions, implementations, criminal prosecutions.	X										Biennially
Data Sharing Agreements	Review of Data Sharing Agreements in place, gaps and processes	X										Biennially
DPIAs	Data Protection Impact Assessments (DPIAs) advice and input by the DPO. Consistency, risks, actions, review.							X				Biennially
Advice (DPO)	Advice provided by the DPO. Risk based advice, data protection obligations, general advice.	X	X	X	X	X	X	X				Annually
Risk Register (DPO)	DPO Risk Register							X				Annually

Appendix C

Data Protection Officer – How Role is discharged

	Data Protection Officer / Organisation Responsibilities	How Practically Discharged	Action / Outputs	Status – June 2019
	Position of the DPO			
1	The DPO must report directly to the highest level of management and is given the required independence to perform their tasks;	• Report to Information Governance Board, SMT, Audit Committee	• DPO report to each IG Board • Quarterly report to SMT • 6-monthly report to ACttee	• In place • To be reviewed • In place
2	The DPO is involved, in a timely manner, in all issues relating to the protection of personal data;	• Regular updates and contact with IG Team as required. • Attendance at IG Team meetings specifically for DPO / GDPR issues	• Ad hoc advice given or information received. • Actions arising for IG Team and/or DPO	• In place • In place
3	The DPO is sufficiently well resourced to be able to perform their tasks;	• Able to utilise IG Team for specific advice and support. • Commission Internal Audit to undertake specific reviews of data protection compliance and general information governance	• Ad hoc advice given or information received. • Internal Audit reports, advice	• In place • Provision included in IA Plan.
4	The DPO is not penalised for performing their tasks;	• Revised contract of employment	• Contract of employment	• In place.
5	The DPO is not required to perform any other duties that result in a conflict of interest with their DPO duties.	• No decision-making responsibilities in relation to data protection policies. • The HoIA role is also independent from operational management and therefore complementary to role of DPO.	• In place – role understood • Declarations of interest raised if necessary	• In place. • In place.
	Tasks of the DPO			
1	The DPO will inform and advise the organisation and its employees about the obligations to comply with the GDPR and other data protection laws;	• Key input/consultee into corporate guidance, POD training, policy development (advisory). • Formal reports to IG Board and Audit Committee • Maintain awareness of developments in data protection law, case law, best practice	• DPO comments, suggestions, advice provided • Reports to each meeting on agreed frequency and ad hoc as required • Monitor ICO website, other articles etc.	• In place • In place • In place. Additional training to be identified and membership of the British Association of DPOs
2	The DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training and undertaking and commissioning audits;	• Programme of audits and reviews undertaken and commissioned through Internal Audit. • Regular meetings with IG Team to be kept aware of current issues • DPO proactively alerted to significant issues by IG Team / SIRO / Caldicott Guardians	• Programme of assurance reviews undertaken • Audit programme planned annually • Formal and informal meeting arrangements • As required	• Completed • In place as part of annual IA planning • In place • In place – as required
3	The organisation will take account of the DPOs advice and the information the DPO provides on data protection obligations;	• Appropriate minutes/record will be taken regarding the advice / reports of the DPO and what action is taken. • DPO has direct and unfettered access to the Chief Executive, SIRO and attendance at SMT as required	• Response to DPO assurance reports and emails in response to queries and advice sought / given • DPO attendance at SMT / meetings with the Chief Executive / SIRO as required	• In place • Review arrangements with new CX July 2019
4	The DPO will provide risk based advice, focussing on the higher risk areas of data processing activities, i.e. where special categories of data are involved;	• DPO consulted on DPIAs (see below) and through liaison arrangements regarding high risk areas	• High risk areas identified by IG Team and IG Board and communicated to DPO through liaison meetings, IG Board etc.	• In place
5	The advice and input of the DPO will be sought when a Data Protection Impact Assessment (DPIA) is undertaken;	• The DPIA process ensures the involvement of the DPO.	• DPO notified of DPIAs required and engaged in process.	• In place

	Data Protection Officer / Organisation Responsibilities	How Practically Discharged	Action / Outputs	Status – June 2019
6	The DPO will also monitor the DPIA process;	• The DPO has access to all DPIAs and will undertake periodic checks to ensure consistency and appropriateness.	• DPIAs to be periodically reviewed as part of DPO assurance reviews or specific internal audits	• As per DPO assurance / audit review programme
7	The DPO acts as a contact point for the ICO, and as such will co-operate with the ICO including during prior consultations under Article 36 (Prior Consultation) and will consult on any other matter;	• The relevant contact details for the DPO have been lodged with the ICO.	• Liaison with ICO as required will be prioritised by DPO and supported by IG Team	• In place
8	The DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purpose of the processing;	• DPO considers and is consulted on the risks associated with processing activities to focus on higher risk areas	• General IG risk register overview by DPO • Data process mapping reviews prioritised	• In place. RR reviewed and will be considered at IG Boards • As per DPO assurance / audit review programme
9	The DPO shall ensure that the organisation documents the reason why any advice given by the DPO is not followed.	• Appropriate minutes / records will be taken regarding the reasons why the advice of the DPO will not be followed.	• DPO will approve how this is recorded in minutes / records should this occur or have his comments recorded.	• Not occurred
	Accessibility of the DPO			
1	The DPO must be accessible as a point of contact for employees, individuals and the ICO	• Within the confines of reasonable working arrangements, the DPO will be available and accessible. • A 'deputy' DPO will be available should the DPO not be so due to annual leave or exceptional circumstances.	• As a senior manager the DPO works flexibly and ensures the regular review of emails etc. • Co-ordination with IG Team in providing 'back-up' arrangements when DPO is not available.	• In place but to review annually • In place but to review in July 2019
2	The contact details of the DPO are published and communicated to the ICO	• The DPO@Barnsley.gov.uk email address is published in all appropriate places.	• Clear reference to DPO and how to contact exists on BMBC website and appropriate policies, procedures etc.	• In place
	Support to the DPO			
1	The DPO is provided adequate resources (sufficient time, financial, infrastructure and where appropriate staff) to enable them to meet their GDPR obligations and to maintain their expert level of knowledge	• The DPO utilises the expertise of the IG Team to assist with GDPR / DPA related matters. • The DPO will have a separate PDR to ensure sufficient focus is given to continuous training and development in data protection matters	• DPO attends IG Team meetings plus ad hoc meetings / discussions as required • PDR from SIRO to ensure focus on professional development and awareness of data protection matters	• In place • To be arranged
2	The DPO must be given appropriate access to personal data and processing activities	• The DPO has unfettered access to all personal data and processing activities in order to discharge his responsibilities and undertake independent and objective audits/reviews.	• Such access formalised in DPA 2018 / GDPR and job profile	• In place
3	The DPO be given appropriate access to other services within the organisations so that essential support, information and input can be received	• The DPO has unfettered access to all senior managers and services in order to discharge his responsibilities to provide support, advice, information, challenge and undertake independent and objective audits / reviews.	• Such access formalised in DPA 2018 / GDPR and job profile	• In place