DRAFT
INTERNAL AUDIT
REPORT SRBC 04/19-20

REVIEW OF GENERAL DATA PROTECTION REGULATION (GDPR)

Issued By: Janice Bamber
Interim Head of Shared Assurance

Lead Auditor: Lisa Hughes

15th January 2020

1	REASONS FOR AUDIT / SCOPE
1.1	On 25th May 2018 the General Data Protection Regulation (GDPR) came into effect, requiring all organisations who process, control and / or store personal data to ensure compliance with the GDPR requirements. The Information Commissioner's Office (ICO) has produced a 12-step plan to assist organisations in achieving compliance, and the Council's current arrangements for GDPR compliance have been measured against this. It should be noted that GDPR is part of the Information Commissioner's Office's Guidance to Data Protection, it does not replace Data Protection principles merely enhances them.
1.2	The introduction and implementation of GDPR provides new risks to the Council, this increased risk was identified as part of the audit planning process and therefore the audit of GDPR was included in the Audit Plan for 2019-20, approved by the Governance Committee on the 14th March 2019. Furthermore, concerns were raised in regard to compliance with GDPR and Data Protection principles by the Interim Chief Executive following his appointment. The concerns identified an increase in the level of risk to the Council, and therefore the scope of the audit has been increased, which has increased the number of days required to complete the audit. It has also resulted in the review covering all areas within the implementation requirement and compliance with the implementation and ongoing principles of GDPR.
1.3	Work undertaken as part of this review focused on identifying the measures implemented to ensure the Council is complying with GDPR. In particular: • Compliance with the ICO's 12 step guide to GDPR implementation • Compliance with GDPR throughout all Council service areas A Gap Analysis has been produced to highlight the work that has been completed with regards to GDPR implementation and clearly shows the areas of GDPR compliance, partial compliance and non-compliance.
1.4	The Gap Analysis is included as item 4 of this report.

2	ASSURANCE RATING
2.1	The review is undertaken in order to form an opinion on the controls in place and the resulting mitigation of risk in respect of the following areas; i. The implementation of GDPR within the Council; ii. Compliance with GDPR principles by all Council service areas
2.2	Internal Audit provide an independent and objective opinion on the adequacy of the Council's control environment, in order to do that Internal Audit review and provide an opinion on the level of assurance of the control environment within each area reviewed. The level of assurance is based on the auditor's assessment of the extent to which system objectives are met, the effectiveness of controls operating within systems and the resultant extent to which risks are mitigated.
2.3	**Implementation of GDPR** The review of processes / procedures in place in respect of the implementation of GDPR has identified that whilst there are some systems of control in place designed to achieve system objectives there are significant weaknesses in the application of controls in this area, as GDPR principles are still not fully implemented some 20 months after the regulations came into effect, leaving the Council open to significant risk. This has resulted in the audit opinion that only Limited Assurance can be placed on the controls in place and the extent to which risks are mitigated in regard to GDPR implementation as there are still a number of areas that do not fully comply with ICO guidance, in particular;

2.4	• Ineffective GDPR Implementation Group; • Ineffective monitoring of GDPR training undertaken; • Lack of awareness and ownership of GDPR across the Council; • Incomplete Record of Processing Activity (ROPA); • Retention Policy not yet fully agreed and adopted; • No formal monitoring system to track and capture records once retention periods have expired; • No formal review of Council Contracts set up prior to the GDPR implementation date, to ensure compliance with GDPR; • A SIRO has yet to be appointed which contravenes the Councils Data Breach Policy and indicates a lack of ownership of GDPR by Senior Management; • There is no defined reporting structure for GDPR matters to Leadership Team again indicating a lack of ownership of GDPR by Senior Management.
2.5	Whilst progress has been made in some areas to ensure compliance with the ICO's 12 step guide, full implementation should have been in place by 25/05/2018, therefore the Council has failed to comply with the requirements of GDPR and until full implementation is achieved the Council remains at risk of data breaches and financial penalties imposed by the ICO.
2.6	**Compliance with GDPR principles** The identification of areas of non-compliance in regard to GDPR principles has resulted in the audit opinion that whilst there are some systems of control in place designed to achieve system objectives, there are significant weaknesses in the application of controls in a number of areas, outlined below, and the extent to which risks are mitigated in those areas. This has resulted in the audit opinion of **Limited Assurance** in regard to compliance with GDPR within all Council services, this is due to the areas of non-compliance as specified above and for the following additional issues which have been identified; • The Data minimisation principle has not been applied to all Council data, thereby breaching GDPR principles; • Personal data is not being held securely in all instances thereby exposing the Council to the risk of unauthorised data access and / or data breaches.
2.7	It was further identified that since GDPR came into effect in May 2018 a total number of 10 Data breaches have been recorded although none of these breaches were of significant impact to warrant being reported to ICO. Whilst all the breaches have been recorded and processed as per the Data Breach Policy, this does highlight an overall lack of awareness and compliance with GDPR.
2.8	**Control Rating Key** **Full –** the Authority can place complete reliance on the controls. No control weaknesses exist. **Substantial** - the Authority can place sufficient reliance on the controls. Only minor control weaknesses exist. **Adequate** - the Authority can place only partial reliance on the controls. Some control issues need to be resolved. **Limited** - the Authority cannot place sufficient reliance on the controls. Substantive control weaknesses exist

3	MANAGEMENT SUMMARY
3.1	The objective of the audit was to review the actions taken by the Council to meet the requirements of and ensure compliance with the General Data Protection Regulation (GDPR) which came into effect on 25th May 2018. The Information Commissioner's Office (ICO) produced a 12-step plan which sets out the actions that should be undertaken, as a minimum, to ensure compliance with the new requirements and the Council's progress in implementation was assessed against this. As well as reviewing relevant documentation and procedures, interviews were held with key staff: The Data Protection Officer (DPO) and Information Asset Owners (IAOs), to establish how each step of the plan has been addressed and the level of understanding of and compliance with GDPR across the Council. **Key Findings** A GDPR Implementation Group, led by The DPO was set up to address the requirements of the ICO's 12 step plan and to assist with GDPR implementation across the Council. Audit found that whilst several of these steps have been actioned and implemented, there are still a number of requirements outstanding, in particular, an approved Retention Policy, adequate training and awareness, and a fully completed Record of Processing Activity (ROPA). The Retention Policy identifies how long certain types of data may be held for and states how data should be destroyed once the retention period has been reached. Without this guidance, there is a risk that data may be held for longer than is necessary which is a breach of GDPR principles. The ROPA is a significant document which identifies all data processed by the Council and

	assigns an Information Asset Owner (IAO) responsible for the management of each data set. The Council was required to meet the GDPR requirements by 25th May 2018, however, the failure to produce these documents means that GDPR is still not fully implemented some 20 months later. Failure to comply with GDPR is a breach of legislative guidelines and exposes the Council to a higher risk of data breaches which in turn leads to reputational damage and could result in financial penalties imposed by the ICO. The audit identified a lack of adequate awareness training. Whilst mandatory training was provided for staff, this was via the Councils e-learning package MILO, which could not be effectively monitored to ensure all staff had undertaken the training or whether it has been effective in providing the necessary awareness. Furthermore, it was identified that Members had not received any GDPR training. Whilst the GDPR implementation group have completed and partially completed areas within the ICO 12 steps guidance for implementation, a number of required policies have not been agreed and issued and GDPR is not fully implemented some 20 months after the required implementation date, therefore the process of implementation has been ineffective.The GDPR Implementation Group has therefore been ineffective in achieving its aims. This has been exacerbated by a lack of priority given to GDPR by Leadership Team. The audit revealed that the Implementation Group was only established in April 2018 and the DPO appointed on the actual date that the new requirements came into effect. Both appointments should have been in place well in advance to mitigate the risks of non-implementation. Further evidence of a lack of ownership by Leadership Team is the failure to define a clear reporting structure to inform Senior Management of the progress / lack of progress being made to implement GDPR. Furthermore, there has been a lack of clarity over the roles of key posts which are essential to good data management, such as the IAOs, DPO and a Senior Information Risk Owner (SIRO). This is further evidenced by the failure to appoint a SIRO in spite of the Council being without one for several months. Whilst discussions with IAOs showed a general awareness of GDPR, it was evident that much reliance was placed on the DPO for adopting processes and completing actions that should be the responsibility of IAOs, specifically the completion of the ROPA. This lack of ownership has hindered the completion process and ultimately led to non-implementation of the GDPR requirements. Additionally, due to the lack of clarity of the roles of IAOs and the DPO, several key tasks have fallen to the DPO to maintain and complete, again showing lack of ownership by IAOs. Discussions with IAOs also revealed that GDPR is not sufficiently embedded throughout the Council. This was further evidenced by a series of walkthrough tests throughout Council offices which confirmed a lack of compliance with GDPR requirements, namely documents containing personal data left out on desks or in unlocked areas and computers left open when unattended, leaving personal data accessible to those who may not be permitted to process it. This is a breach of the GDPR's security principle which stipulates the importance of protecting personal data and ensuring that organisations must protect data against unauthorised or unlawful processing. The audit identified that a total of 10 Data Breaches have been recorded since GDPR came into effect in May 2018 and whilst none of these were of significant impact to warrant being reported to the ICO, this does highlight a lack of awareness and compliance with GDPR which puts the Council at risk of legislative, financial and reputational damage.

4. General Data Protection Regulation Gap Analysis re ICO's 12 steps Guidance

GDPR Requirements **ICO 12 Step Guidance**	Findings	Compliant	Management Action
The ICO states that:-			
Awareness			
You should make sure that Decision Makers and key people within your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.	All staff within the Council were required to complete on line mandatory training via the Council's MILO system. The audit identified that the e-learning system was unable to produce records to confirm that all members of staff had completed the training. It was also identified that Members have not been provided with any GDPR training. A GDPR group was established with representation from each service area, testing confirmed that the group meets on a regular monthly basis, this is to change to fortnightly until implementation is completed; Whist the GDPR group have met regularly over the last 20 months, the group was established as an implementation group, testing of the status against the 12 step requirements has identified that not all steps have been completed, a number of required policies have not been agreed and issued and GDPR is not fully implemented some 20 months after the required implementation date, therefore the process of implementation has been ineffective. The Data Protection Officer (DPO) has attended some team briefs to update on GDPR requirements and continue to raise awareness. GDPR has been added to the Team Brief standing items as a requirement, however, it is not currently a standing item on the Leadership Team agenda. GDPR is published on the Council's Intranet pages, Blogs are maintained and posters promoting privacy have been observed around the buildings in order to raise further awareness. Information Asset Owners confirmed awareness that matters relating to GDPR should be referred to the DPO.	P	MA1 & MA2
Information Held			
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit	It was identified that a Record of Processing Activities (ROPA) has been created. Whilst this has been set up to contain all the required detail as per GDPR requirements, it is not yet fully complete and does not therefore identify all processing activities. Audit testing showed that whilst IAOs were aware of the requirement to complete a ROPA, this task had been coordinated by the DPO and not completed by IAOs. There is a general failure of IAOs to own the data processes thereby hindering the completion of the ROPA, expecting the DPO to take responsibility for its completion. A draft Retention Policy has been prepared but is still awaiting approval and is yet to be implemented. The policy will include the retention periods for each service when finalised, however the audit identified that there is no formal monitoring system in place to track data records once retention periods have expired. The policy explains that 'records' include paper, electronic, microform and audio-visual formats. The Policy does not however include instructions for keeping disposal records. The Privacy Notice detailed on the Council's Website also lists retention periods for each service area. Systems are in place to ensure staff emails are automatically deleted after 2 years. For most staff this is 2 years but for senior staff this can be up to 7 years. The audit identified that prior to the GDPR implementation date, the Council's suite of 'template standard conditions of contract' was updated to take account of GDPR, and details of this were posted on CONNECT advising contract managers to review their existing contracts re adding further detail. However, there was no follow up as to whether this was done, and it cannot therefore be confirmed whether contract set up prior to the GDPR implementation date comply with the requirements.	N	MA3, MA4, MA5, MA6 & MA7

Communicating Privacy Information			
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.	The Council's Privacy Notice is publicly accessible on its website and details the purposes for processing data, who it may be shared with, how long it will be kept and the lawful basis for processing. Service specific details are included within this and each shows the lawful basis for processing. When accessing Services on the Council Website, the Privacy Notice is displayed to the user as an automatic pop up.	Y	
Individuals' Rights			
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.	The privacy policy is accessible on the Council Website lists all an Individuals' rights and explains that customers should contact the Council if they wish to exercise any of their rights. The Data Protection Policy has also been updated to include Individuals Rights and GDPR Principles and is accessible for staff via CONNECT. The MILO training also explains Individuals' Rights, including the Right to Erasure. Audit testing confirmed that there is a software package for recording requests relating to Individuals' rights, which is maintained by the DPO. IAOs also confirmed that they were aware of the Individual Rights and would refer any requests to the DPO. It was also confirmed that once files are deleted from IT systems, they are put 'beyond use' and do not remain on back up systems. The draft Retention Policy has been reviewed and includes methods for deleting information, however, this is still only a draft and has yet to be approved and implemented.	P	MA3 & MA9
Subject Access Requests			
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.	Individuals Rights, including Subject Access Requests (SAR) are detailed in the updated Data Protection Policy, which is in line with GDPR requirements and explains that requests must be responded to within 1 month. Guidance for staff on how to respond to a SAR is also available on CONNECT in the GDPR section, under Information Requests Procedures. In line with GDPR requirements, the procedures explain that requests may be verbal or in writing. They also state that requests will be logged and timescales for response monitored by Information Services.	Y	MA10
Lawful Basis for processing personal data			
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.	Managers have updated the Privacy Notices for each of their services, and these are available on the Council's website. The information included states the lawful basis for processing and provides the relevant legislation that permits processing. The lawful basis for processing is also detailed within the ROPA document although this is yet to be finalised.	P	MA3
Consent			
You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.	Consent is rarely the lawful basis used for the processing of data within the Council, however it was identified that consent forms are required for the use of photographs or filming at events. A consent form has been devised which adheres to GDPR regulations and copies of completed forms are held securely. However, it is unclear whether all services area aware of the procedure to follow for obtaining consent.	P	MA11
Children's Data			
You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental consent for any data processing activity	There are currently no services provided directly to children. The Council provides sports development services to schools but in these instances, the school holds the data.	N/A	

Data Breaches			
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.	A Data Breach Policy has been implemented (Apr 2019) and is listed on CONNECT under GDPR Policies. Testing identified that all reported breaches are listed on a Data Breach Tracking Log by the DPO and records of the completed Data Breach Form, and where relevant a copy of the ICO self-assessment result, are retained. The Data Breach policy refers to the Senior Information Risk Owner (SIRO), who 'has responsibility at executive level for oversight of data protection' however, the Council does not currently have a SIRO in post. Staff are made aware of individual training and policies via CONNECT but there is no specific monitoring of whether they have completed courses or read policies. The Council does not currently hold any cyber insurance or insurance to cover against costs associated with data breaches.	P	MA2, MA12, MA13 & MA14
Data Protection by Design and Data Protection Impact Assessments (DPIA)			
You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party and work out how and when to implement them in your organisation.	DPIA guidance is available on CONNECT. However, there is no direct link to this within the GDPR section of CONNECT. The audit confirmed that IAOs were aware of the DPIA process although they had not received training regarding this.	P	MA2, MA13 & MA15
Data Protection Officers			
You should designate someone to take responsibility for data protection compliance and assess where the role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.	The Council has a designated DPO who is a certified GDPR Practitioner and has been in the role since 25/5/18. This role is a specified role as per GDPR requirements and although the requirement has been met, the role should have been filled considerably sooner to ensure Council compliance by the GDPR implementation date. The Data Protection Policy explains that the DPO has specific responsibility for Data Protection within the organisation. The DPO chairs the GDPR Implementation Group which has devised an Action Plan of tasks required to ensure GDPR compliance. However, given that the Council are still not yet fully compliant with implementation or the ICO 12 steps for implementation, the Council have failed to comply with GDPR. The DPO has various other duties aside from Data Protection, and has assistance one day a week from another officer for GDPR tasks. GDPR is not a standing item on SLT agendas and therefore is not always discussed highlighting a failure of Leadership Team to take ownership of GDPR. The procedures and steps being taken to demonstrate the Council's compliance are documented, as per the GDPR Accountability Principle. The ROPA document includes the required detail as stated in ICO guidance, however, this is still in draft format and has yet to be approved and implemented. Measures are in place to record any requests received re Individuals Rights. SARs are recorded on a database held by Information Services and the Retention Policy and Special Data policies have been written and are currently awaiting SLT approval.	P	MA1, MA3, MA12, MA16 & MA17
International			
If your organisation operates in more than one EU member state (i.e. you carry out cross border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.	This is not applicable to the Council. The information obtained from Heads of Service/Directors to compile the Asset Register and ROPA shows that there are no areas operating outside the UK.	N/A	

5. MANAGEMENT ACTION PLAN

NO.	CONTROL ISSUES / RISKS	PROPOSED MANAGEMENT ACTIONS	AGREED ACTIONS	OFFICER & DATE
	Awareness			
1	Whilst the GDPR Group meet regularly they were originally set up as the GDPR Implementation Group, given that GDPR is still not yet fully implemented some 20 months after the implementation date, the group has been ineffective in fully implementing GDPR and ensuring GDPR compliance with the principles. This is a breach of GDPR principles and leaves the Council exposed to the risk of data breaches which in turn could cause reputational harm and/or financial loss should ICO impose financial penalties. In addition, this exposes the Council to ICO inspection which again could cause reputational harm and/or financial loss.	**To renew the focus and commitment of the GDPR Group, agreeing clear terms of reference and an action plan to ensure the group are more effectively utilised in implementing and monitoring compliance with GDPR.**		
2	There is no effective monitoring process in place to ensure all staff have completed the appropriate GDPR training. In addition, Members have not yet received any GDPR training, despite the GDPR implementation date of 25/5/18. There is a risk that policies and procedures are not sufficiently understood by staff and Members and therefore a lack of awareness of the requirements of GDPR. Although some mandatory GDPR training has been provided to staff through the MILO e-learning package this has not been effectively monitored so cannot be verified that all staff have undertaken this training or whether it has been effective in providing the necessary awareness. There is a risk that awareness of GDPR throughout the Council has not been achieved, leaving the Council exposed to the threat of data breaches, reputational harm and financial loss.	**A review of GDPR training requirements must be undertaken and any training needs addressed. All GDPR training must be clearly monitored and recorded to ensure appropriate GDPR training is completed by all staff and Members and policies and procedures have been understood.**		

	Information Held			
3	A Register of Processing Activity (ROPA) has been set up which includes columns for all required information re ICO guidance, however this is only partially complete, and does not therefore identify all processing activities. There has been a general failure of Asset Owners / Senior Management to take ownership of the GDPR data processes thereby hindering the completion of GDPR documentation and procedures with the expectation that the DPO will take responsibility for completion of documents rather than the asset owners. There is a risk of non-compliance with GDPR principles which leaves the Council exposed to data breaches which in turn could cause reputational harm and/or financial loss should ICO impose financial penalties.	**The responsibilities of Data Owners are to be clearly re-iterated to Officers ensuring that they understand the requirements of GDPR processes and complete the required documentation to ensure full implementation and compliance with GDPR, this must include as a minimum;** - **A fully completed ROPA identifying all processing activity;** - **An approved Retention Policy and retention schedules.** **Both documents are to be formally adopted as a matter of urgency.**		
4	Emails are retained in most cases for two years before automatic deletion, although for some staff these are held for up to seven years. There is a risk that records are retained for longer than is necessary which is a breach of GDPR principles.	**The Council must consider reviewing its email retention policy to ensure data is not held longer than necessary.**		
5	A draft Retention Policy has been completed but does not include instructions for keeping disposal records as per the ICO's FOI guidance – Section 46. A Retention Policy has not yet been fully agreed and adopted, in addition there is no formal monitoring system to track and capture records once retention periods have expired. There is a risk that records are retained for longer than is necessary which is a breach of GDPR principles.	**The draft Retention Policy should include reference to what disposal records should be kept as per the FOI guidance.** **(Also see MA3).**		

6	Interviews with Information Asset Owners (IAOs) revealed that there are no set procedures in place for ensuring records are deleted once the retention period has expired. Records are deleted as and when time allows which poses the risk that information is held for longer than is necessary which is a breach of GDPR principles.	**A formal monitoring system must be implemented across the Council to ensure that records are deleted once the retention period date has expired.**		
7	The Procurement Team has updated the Council's suite of 'template standard conditions of contract' to take account of GDPR and staff were advised via CONNECT to consider these when setting up new contracts. Legal Team also compiled a full register of contracts held by the Council. However, there was no review of existing contracts by either service to ensure they complied with GDPR. Not all existing Council contracts have been reviewed to ensure they comply with GDPR principles. There is a risk that contracts which existed prior to the GDPR implementation date do not take account of GDPR principles and therefore breach GDPR rules. This exposes the Council to the risk of data breaches which in turn could cause reputational harm and/or financial loss should ICO impose financial penalties.	**Contracts set up prior to the GDPR implementation date must be reviewed, to ensure that they comply with GDPR requirements.**		
8	Interviews with IAOs revealed that several Departments across the Council use paper records which hold personal data. This increases the risk of unauthorised data access and/or data breaches leading to reputational harm and/or financial loss should ICO impose financial penalties.	**Where possible paper records should be scanned and held electronically.**		
	Individuals' Rights			
9	Individuals' Rights are explained within the Data Protection Policy, but there are no specific written procedures for staff for dealing with customer requests relating to these. However, this is because the current procedure is to refer all requests to the DPO to action.	**The Council should consider whether full reliance on the DPO is acceptable or whether individual services should manage their own requests.**		

	Subject Access Requests (SARs)			
10	Information Request Procedures and a Subject Access Request form are held on CONNECT under Information Services. However, these have been superseded by ones written to comply with GDPR which are located under the GDPR section. There is a risk that incorrect forms/procedures are used by staff which may contravene GDPR principles.	**A review of guidance and procedures listed under Information Services must be undertaken and any obsolete documents/guidance deleted to ensure there is no conflicting information.**		
	Consent			
11	Photography and filming of the public at Council run events has been identified as an area where the Council need to obtain consent. Consent forms have been devised and are GDPR compliant, however it is not clear whether all services who host events are using these. There is a risk of GDPR non-compliance which exposes the Council to reputational harm and/or financial loss.	**Guidance for obtaining consent for filming and photography, and where necessary setting up contracts, must be documented and posted on CONNECT. Officers responsibilities with regard to obtaining consent must be reiterated to all staff.**		
	Data Breaches			
12	A Data Breach policy has been produced which refers to the SIRO who 'has responsibility at executive level for oversight of data protection'. However, there is currently no SIRO appointed within the Council, which is a breach of our Data Breach Policy and shows a failure of the Leadership Team to take ownership of GDPR and clarify the roles of officers, the DPO and SIRO with regards to Data Protection.	**Leadership are to take ownership of GDPR and clarify the roles of officers namely; SIRO, DPO and Data Owners.**		
13	Policies and procedures relating to GDPR have been produced e.g. Data Security, Data Breaches, SARs. However, there is no monitoring system in place to ensure these have been read and understood by all staff and Members. There is a risk that Officers and / or Members do not fully understand the principles of GDPR which exposes the Council to possible data breaches thereby causing reputational harm and / or financial loss.	**A review of GDPR training requirements must be undertaken and any training needs addressed. All GDPR training must be clearly monitored and recorded to ensure appropriate GDPR training is completed by all staff and Members and policies and procedures have been understood.** **(As per MA2)**		
14	There is currently no insurance policy in place to protect the Council against costs associated with data breaches. This	**Whilst an appraisal has been undertaken and deemed not**		

	poses a financial risk to the Council should we receive a financial penalty following a data breach.	**necessary at this stage a regular re-appraisal must be undertaken to assess the risk to the Council against the cost of insuring.**		
	Data Protection Impact Assessments (DPIAs)			
15	An article regarding DPIAs was posted on CONNECT with links to guidance attached. However, this information is not easily accessible as it is not located within the GDPR area of CONNECT.	**The DPIA form and guidance must be moved to the GDPR area of CONNECT and staff notified that the information is there.**		
	Data Protection Officer			
16	The Council has appointed a DPO who is responsible for ensuring data protection compliance and monitoring compliance with GDPR. However, the DPO is not a dedicated role and has an additional role as the Head of Customer Experience. ICO guidance states that the DPO shouldn't be expected to manage competing objectives that could result in data protection taking a secondary role. There is a risk of non-compliance with GDPR principles which leaves the Council exposed to data breaches which in turn could cause reputational harm and/or financial loss should ICO impose financial penalties.	**In view of the fact that GDPR is still not fully implemented within the Council, senior management must consider whether more resources should be assigned to assist the DPO in his duties.**		
17	ICO guidance also states that the DPO must report to the highest management level. Whilst one to one meetings are held fortnightly with the Director of Customer and Digital, there is no defined reporting structure to SLT. This is a breach of ICO guidance and indicates a failure of the Leadership Team to take ownership of Data Protection.	**A system must be in place to ensure that Data Protection and GDPR matters are regularly reported to SLT either by the DPO or the Director of Customer and Digital.**		
	Data Minimisation Principle (compliance)			
18	To comply with the Data Minimisation Principle, the Council must ensure that the data it holds is adequate, relevant and limited to what is necessary for its processing purposes. Interviews with IAOs revealed that the majority of services	**Each service area is to undertake a review of the data it holds to ensure it is not holding any unnecessary data. Any data which does not**		

	have not undertaken any recent review of the data they hold to ensure that they comply with this principle. The Council cannot verify that all the data it holds is adequate, relevant and limited to what is necessary for its processing purposes. (Data Minimisation Principle) This exposes the Council to the risk of data breaches and non-compliance with the Data Minimisation Principle which in turn could cause reputational harm and/or financial loss should ICO impose financial penalties.	**comply with the GDPR principles must be disposed of.**		
	Data Protection (compliance)			
19	The results of walkthrough testing around Council offices revealed that paper documents containing personal data are being left on desks and in unlocked areas, therefore personal data is not being held securely in all instances, which is a breach of GDPR principles. This exposes the Council to the risk of unauthorised data access and/or data breaches leading to reputational harm and/or financial loss should ICO impose financial penalties.	**Directors/Assistant Directors must ensure that all teams are aware of the requirement to store personal data documents securely when not in use.**		

A lack of timely implementation of the agreed actions may be reported to the Governance Committee.

All internal audit work is conducted in compliance with the Public Sector Internal Audit Standards, issued by the Chartered Institute of Public Finance and Accountancy and the Chartered Institute of Internal Auditors.

Statement of Responsibility

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.