Bury Metropolitan Borough Council

Data protection audit report

July 2021

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

Bury Metropolitan Borough Council (BMBC) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 23 March 2021 with representatives of BMBC to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and BMBC with an independent assurance of the extent to which BMBC, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of BMBC processing of personal data and Freedom of Information requests. The scope may take into account any data protection issues or risks which are specific to BMBC, identified from ICO intelligence or BMBC's own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of BMBC, the

nature and extent of BMBC's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to BMBC.
It was agreed that the audit would focus on the following area(s)

Scope area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Information Security	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
Freedom of Information	The extent to which FOI/EIR accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and in operation throughout the organisation.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, BMBC agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 22 June to 24 June 2021 The ICO would like to thank BMBC for its flexibility and commitment to the audit during difficult and challenging circumstances.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection and freedom of information legislation. In order to assist

BMBC in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. BMBC'S priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

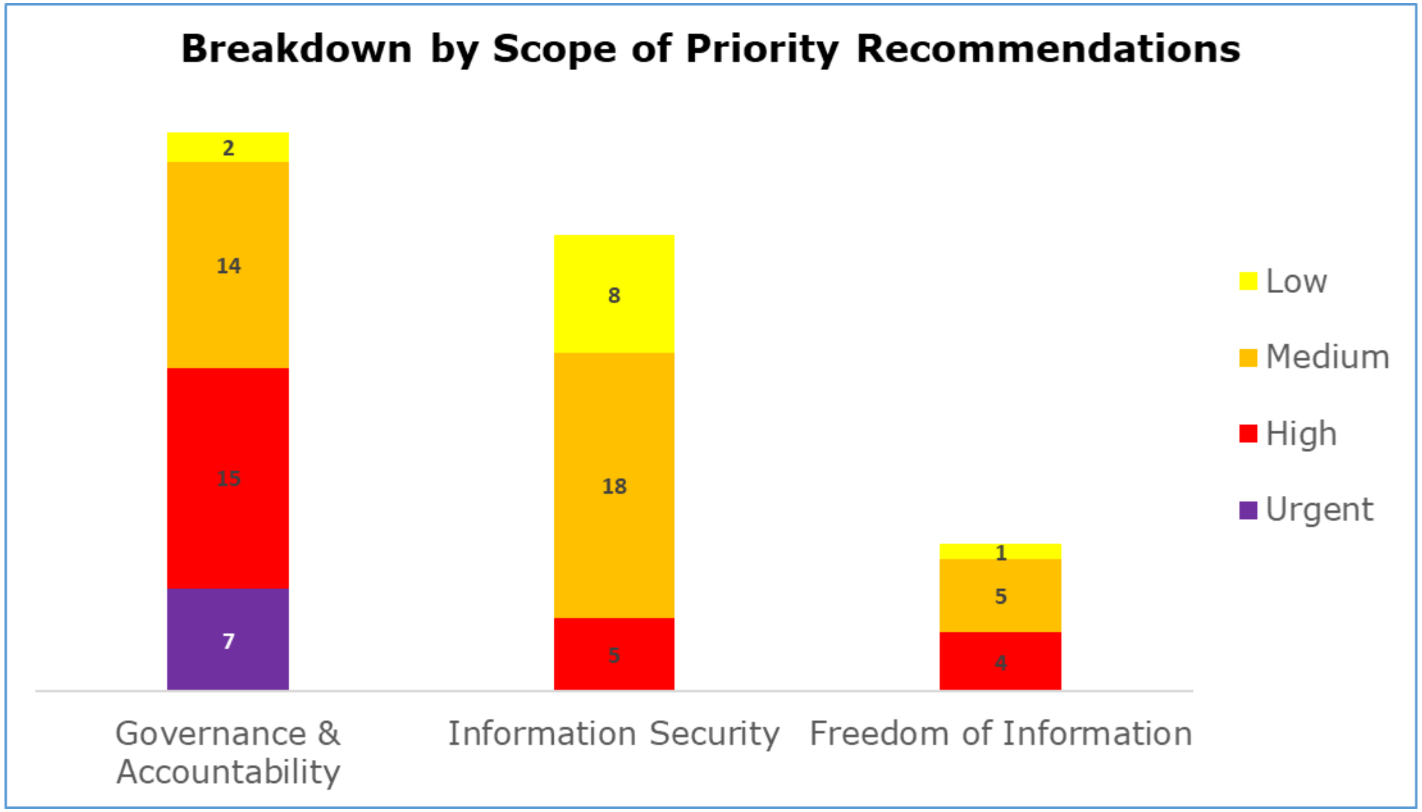
Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Information Security	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Freedom of Information	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering freedom of information compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with freedom of information legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations

A bar chart showing a breakdown by scope area of the priorities assigned to the recommendations made.



The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance & Accountability has seven urgent, 15 high, 14 medium and two low priority recommendations
- Information Security has five high, 18 medium and eight low priority recommendations
- Freedom of Information has four high, five medium and one low priority recommendations

Areas for Improvement

BMBC does not currently maintain a central log of its lawful bases for processing, meaning there is no oversight on whether the appropriate lawful basis is being used. BMBC should establish a central log of lawful bases, including details of any law, statute, or other obligation for that processing.

The Records of Processing Activities (RoPA) held by BMBC does not include certain categories of information required by the UK GDPR. BMBC should ensure that its RoPA is updated to include all details specified by the legislation.

BMBC does not have a Legitimate Interests Assessment (LIA) in place for the processing it carries out under the lawful basis of Legitimate Interest. BMBC should undertake an LIA on this processing to ensure it has adequately balanced its interests against the rights and freedoms of the data subject.

BMBC should gain assurance from suppliers that they will notify BMBC within a reasonable timeframe of any information security breaches or personal data breaches. All breaches should be notified to a nominated person.

BMBC should separate out the key elements of FOI/EIR legislation from the existing Data Protection eLearning module to create a new FOI module. Use the new module for mandatory FOI induction and refresher training for all staff.

A specialist training programme should be created for all those staff with responsibility for responding to FOI/EIR requests. The training should be recorded and refreshed on a regular basis.

BMBC should review the existing FOI pages on the council web site to demonstrate and ensure compliance with current guidance whilst ensuring the benefits gained from the web request form are not diminished.

Best Practice

BMBC have integrated communications around information governance into weekly executive emails, ensuring data protection matters are visible to all levels of staff.

Departments hold a library of responses to frequent FOI/EIR requests to reduce workload, reduce response times and capitalise on any effort already expended on similar requests.

BMBC has metacompliance software in place to ensure all staff have read and completed the Personal Commitment Statement. The statement outlines key information security requirements that staff must follow

Audit findings

The tables below identify areas for improvement that were identified in the course of our audit; they include recommendations in relation to how those improvements might be achieved.

Governance & Accountability

Control	Non-conformity	Recommendation	Priority
There is a Data Protection Officer in place with designated responsibility for data protection compliance.	a.1.A. There is a blurring of responsibilities between the Deputy Director of Governance and Assurance (DDGA) at Bury CCG, and BMBC's DPO. There is a confusion on expectations - it was reported to ICO auditors that the DDGA carries out the operational aspects of IG and DP and the DPO sits in a statutory role, however separately the DDGA was described as a specialist advisor to help implement measures but not run them. There is a risk that areas of DPO responsibility as delegated in Articles 37, 38, and 39 of the UK GDPR will be missed as there are not clear lines on who is responsible for them. B. See a.3. C. The DPO is not sufficiently well-resourced. There is no DP or IG department, and as a result	a.1.A. Clear delineation between the DPO's role and the advisory position of the DDGA is required. BMBC needs to clarify exactly what is required of a DPO by the UK GDPR and ensure its DPO is fulfilling those duties, then it will be able to provide clarity on whether the DPO or DDGA is responsible for specific aspects of DP or IG. This will ensure BMBC is fulfilling its obligations under Articles 37, 38, and 39 of the UK GDPR. B. see a.3. C. BMBC have plans in place to adequately resource IG projects and should implement them as soon as they are reasonably able to do so. By ensuring that there are specialised staff available to assist in responding to	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	many operational aspects of IG, such as responding to individual rights requests, is managed within services. BMBC have advised of resourcing plans that were put on hold due to the pandemic. There is a risk that the DPO is prevented from carrying out their role effectively, due to lack of resourcing.	individual rights requests, or provide help and guidance on data protection matters, the DPO will be able to carry out their role effectively.	
The DPO role has operational independence and appropriate reporting mechanisms are in place to senior management	a.2. BMBC's DPO also holds many other roles, including Head of Legal Services and Deputy Monitoring Officer. By holding several senior management roles, BMBC is unable to provide assurance that its DPO has operational independence and that there is no conflict with the DPO's numerous other duties as part of their role. This could result in non-compliance with Article 38(6) of the UK GDPR, which highlights that whilst DPOs may fulfil other tasks or duties, "the controller or processor shall ensure that any such tasks and duties do not result in a conflict of interest".	a.2. BMBC should consider creating documentation to account for the possibility of a conflict of interest arising, and the backup reporting measures in place to mitigate this risk, e.g. designating responsibility to another staff member on matters which could be perceived as a conflict of interest for the DPO. This will ensure BMBC can demonstrate compliance with Article 38(6) of the UK GDPR.	Medium
Operational roles and responsibilities have been assigned to support the day to day management of all aspects of information governance	a.3. The responsibility for day-to-day management of IG is not centralised or standardised - each department manages their duties individually, so there are no processes in place to ensure the DPO is involved in DP issues in a timely manner. There is no oversight by the DPO on individual department IG management and performance. ICO Auditors were advised that there is a network of IG leads, although this was unable to be evidenced, and there have previously been DP champions in departments but this has not been maintained due to the pandemic. This means there are no assurances the correct staff are in place and are trained	a.3. BMBC should implement processes to ensure the DPO has oversight of IG management and performance across individual departments. BMBC should consider reinstating DP champions and facilitating DP champion meetings in and across departments. This will allow good practice and lessons learnt to be shared across departments and provide an opportunity for the DPO to attend to ask and answer any questions there may be around the operational aspects of IG. This will ensure that the correct staff are in place and	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	accordingly, or that BMBC is fulfilling its obligations under the UK GDPR.	that BMBC is fulfilling its obligations under the UK GDPR.	
There are processes in place to ensure information risks are managed throughout the organisation in a structured way.	a.4. A mixed awareness of risk registers was reported to ICO auditors, with some departments confirming they held their own register and others stating they were only aware of the corporate register. Without the appropriate oversight of information risks across the organisation, BMBC does not have adequate assurance they are preventing misuse of personal data, which may result in a personal data breach or non-compliance with their obligations under the UK GDPR.	a.4.Document where departmental risk registers exist and commence enquiries into where they don't and why. BMBC should ensure that all departments are aware of their risk registers, and that ownership is allocated to a suitable staff member. This will mitigate the risk of misuse of personal data and ensure BMBC are in compliance with their obligations under the UK GDPR.	Urgent
There are local level operational meetings where data protection, records management and information security matters are discussed.	See a.3.	See a.3.	
Management support and direction for data protection compliance is set out in a framework of policies and procedures.	a.5.A. Policies and procedures relating to data protection matters are in place. However, these documents are significantly out of date and have not been updated and reviewed for a number of years. There is a risk that breaches will occur as the policies and procedures do not meet the requirements of the UK GDPR and DPA18. B. BMBC does not currently have a specific individual rights policy. As a result, there is a risk that individual rights requests will not be recognised as they are not documented anywhere or included in any specific training. In addition, there is a risk BMBC will not fulfil its	a.5.A. Policies and procedures should be reviewed and updated to reflect the new requirements on controllers detailed in the UK GDPR. This will ensure that BMBC is accurately reflecting its obligations under the updated legislations. B. Implement an individual rights policy, including details on what rights individuals have, exemptions that can be applied, and how requests can be made. This will ensure BMBC fulfils its obligations under Articles 12-23 of the UK GDPR.	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	obligations under Articles 12-23 of the UK GDPR, which set out the rights of the individual.		
Where the organisation is required by Schedule 1 or Part 3 section 42 of the DPA18 to have an Appropriate Policy Document (APD) in place, the document in place is sufficient to fulfil the requirement.	a.6. No document that would constitute an Appropriate Policy Document (APD) has been provided to ICO auditors. As such, BMBC has no assurance that it has properly considered and documented their justification for processing special category or criminal offence data as required under Part 3 Section 42 or Schedule 1 of the DPA18.	a.6. BMBC must implement an APD to support the accuracy of the decisions made to process special category or criminal offence data. This will ensure BMBC meets the requirements of Part 3 Section 42 or Schedule 1 of the DPA18.	Urgent
Policies and procedures are approved by senior management and subject to routine review to ensure they remain fit-for-purpose.	a.7.A. Evidence provided to ICO auditors shows that there is no consistent document control information on policies or procedures, meaning there is no way of determining whether a document is the most recent version, or requires review. There is no accountability when it comes to ensuring documents are routinely reviewed and updated. This means BMBC is not compliant with Article 5(2) of the UK GDPR, the Accountability principle. B. BMBC does not have a formal, documented policy review process - there is no set procedure for reviewing, ratifying and approving new or updated policies. This means there is no assurance around the effectiveness of policies and procedures, and that BMBC is not compliant with Article 5(2) of the UK GDPR, the Accountability principle. C. There is no centralised policy review schedule, so there is no accountability or assurance around ensuring documents are routinely reviewed and	a.7.A. All policies, procedures and guidelines should be updated to include document control information - at minimum, this should include version number, document owner, change history, and review date. This will give ownership and accountability to policies and ensure BMBC's compliance with Article 5(2) of the UK GDPR. B. BMBC should create a formal, documented policy review process, to ensure a standardised approach to reviewing, ratifying, and approving new or updated policies. This will provide assurance around the effectiveness of policies and procedures and ensure BMBC's compliance with Article 5(2) of the UK GDPR. C. BMBC should formulate a centralised policy review schedule, to provide accountability and assurance around documents being routinely reviewed and	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	updated. This means BMBC is not compliant with Article 5(2) of the UK GDPR.	updated. This will ensure BMBC's compliance with Article 5(2) of the UK GDPR.	
Policies and procedures are readily available to staff and are communicated through various channels to maintain staff awareness	a.8. There is a lack of oversight on ensuring staff without computer access have copies of policies and procedures available to them. There are no measures in place to make sure that this is the case, as it is down to individual managers to take responsibility for documents being available. There is an uncontrolled risk that staff will act without reference to guidance, and in breach of the UK GDPR or DPA18 - meaning BMBC is not conforming to the requirements of Article 5 of the UK GDPR, the Data Protection Principles.	a.8. BMBC should ensure the relevant DP and IG policies and procedures are available to all staff without computer access - for example creating a document bundle retained by depots or offices that contains the appropriate information. This will allow staff to reference guidance as required and ensure BMBC conforms to the Data Protection Principles set out in Article 5.	Medium
There is an overarching IG training programme in place for all staff.	See c.9.	See c.9.	
Induction training is in place and delivered in a timely manner to all staff including temporary and agency staff etc.	a.9. Induction training at BMBC includes the basic GDPR training, and a requirement to read the relevant data protection policies. However, there is little assurance that staff have completed training before being granted access to systems that process or hold personal data. There is a risk of non-compliance with the Data Protection Principles, set out in Article 5(1) of the UK GDPR.	a.9. Regular reporting should be carried out on who has access to systems containing personal data, and who has completed the mandatory GDPR training. This will allow BMBC to identify if any staff who have not completed the mandatory training have access to systems holding or processing personal data. Where staff have not completed the training, access should be rescinded until the training is complete. Where the staff member is a new starter, a report should be run to confirm training has been completed before granting access to these systems. This will ensure BMBC is in compliance with Article 5(1) of the UK GDPR.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is provision of more specific DP training for specialised roles (such as the DPO, SIRO, IAOs) or particular functions e.g. records management teams, SAR teams, information security teams etc.	a.10.A. The DPO has not undertaken any specific DP or IG training and cannot evidence any DP or IG certifications to qualify them for the role. Whilst Article 37(5) of the UK GDPR does not specify any qualifications a DPO should hold, it is expected that a DPO should be able to evidence their "expert knowledge of data protection law and practices". Failure to have an appropriately qualified DPO may be a breach of Article 37 of the UK GDPR. B. There is no provision of specific DP training for specialised roles or particular functions - for example Information Asset Officers (IAOs) do not have specific training on their role and its responsibilities, and there is no specialised training in how to recognise or respond to a SAR. This leaves BMBC at risk of not meeting its obligations under the UK GDPR and DPA18.	a.10.A. BMBC should facilitate the DPO attending specific, specialised DP or IG training, in order to evidence and maintain their expert knowledge, and ensure BMBC is complying with their obligations under Article 37. B. The requirement for staff in particular roles or functions to have more specific training was highlighted in BMBC's recent Training Needs Analysis (TNA). BMBC should implement a specialised training programme to meet the needs of staff in these roles - i.e. what the role and responsibilities of an IAO are, how front line staff can recognise and process a SAR. This would ensure BMBC is meeting its obligations under the UK GDPR and DPA18.	High
The organisation has considered a programme of external audit with a view to enhancing the control environment in place around data handling and information assurance	a.11. BMBC does not engage an external auditor to provide independent assurances on IG practices. External auditors are engaged for the purposes of information security only. By only assessing risk through internal audits and assurances, BMBC are at risk of inaccuracies in risk assessments and potential breaches, and non-conformance with Article 5(1) of the UK GDPR, the Data Protection Principles.	a.11. BMBC should consider engaging an external auditor to provide an independent view on its IG practices. This will provide additional assurances and cover any potential blind spots, to minimise risk of inaccurate risk assessments or any potential breaches. It will also provide additional layers of assurance that BMBC is conforming with the Data Protection Principles detailed in Article 5(1) of the UK GDPR.	Medium
There is a programme of risk- based internal audit in place covering information governance / data protection.	a.12. Data protection matters are included within the scope of all audits in BMBC's internal audit plan. However, BMBC does not routinely conduct internal audits solely around data protection compliance, and the DPO is not included in audit	a.12. BMBC should routinely conduct internal audits covering a range of data protection compliance areas. This will ensure BMBC and its DPO have continuous oversight and assurance that it is maintaining compliance	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	planning. This means BMBC and its DPO may be lacking oversight and assurance that it is maintaining compliance with its obligations under the UK GDPR and DPA18.	with its obligations under the UK GDPR and DPA18.	
The organisation actively monitors or audits its own compliance with the requirements set out in its data protection policies and procedures.	a.13. BMBC's data protection policies and procedures do not specify what the compliance monitoring process is, to ensure staff are adhering to policies. Without ongoing compliance monitoring, BMBC lacks assurance that the controls it has in place to prevent non-compliance with the UK GDPR and DPA18 are being implemented.	a.13. Establish within data protection policies and procedures how compliance will be monitored. By continuously monitoring staff compliance with policies and procedures, BMBC will have ongoing assurance that the controls it has created are being implemented correctly and preventing non-compliance with the UK GDPR and DPA18.	Medium
There are data protection Key Performance Indicators (KPI) in place	a.14. BMBC has recently implemented KPIs for FOI and SAR completion. However, there are no KPIs relating to data protection training, information security, or records management. Without KPIs in place, BMBC lacks oversight on its compliance with its statutory obligations and cannot demonstrate compliance with Article 5(2) of the UK GDPR, the Accountability principle.	a.14. BMBC should implement or expand their KPIs in the following areas: -Individual rights requests, to include breakdown by type of request, and area the request was received -Data protection training, including percentage of staff completing mandatory training -Information security, including number of security breaches, incidents, and near misses -Records management, including use of metrics such as file retrieval statistics, adherence to disposal schedules, and performance of systems in place to index and track paper files containing personal data. This will ensure that BMBC has oversight on its compliance with statutory obligations and can demonstrate accountability as required under Article 5(2) of the UK GDPR.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
Performance to IG KPIs is reported and reviewed regularly.	See a.14.	See a.14.	
There are written contracts in place with every processor acting on behalf of the organisation which set out the details of the processing	a.15. BMBC does not have a central contract log for data processors - this is managed within services. This means there is no oversight of processor contracts by the DPO, and no assurance that contract reviews are taking place regularly and consistently.	a.15. BMBC should create a central log for data processor contracts. This will provide oversight on processor contracts by the DPO and provide assurance that contract reviews take place regularly and consistently.	High
Written contracts include all the details, terms and clauses required under the UKGDPR	a.16. Evidence provided to ICO auditors indicated that details of processing - e.g. the subject matter, the duration, the nature and purpose, the type of personal data - is not included as standard in a processor contract, as required by Article 28(3) of the UK GDPR. There is a risk that BMBC may lose control of personal data, resulting in a breach, or that BMBC may be unable to respond to individual rights requests within the statutory timeframe. There is also non-compliance with Article 5(2) of the UK GDPR, the Accountability principle.	a.16. BMBC should ensure that the categories of information set out in Article 28(3) of the UK GDPR are included in all processor contracts - consider implementing a standard contract in order to achieve this. Once contracts have been updated, BMBC should ensure that compliance checks are carried out on updated contracts. This reduces the risk that BMBC may lose control of personal data or be unable to respond to individual rights requests within the timeframe designated by the UK GDPR. This will also ensure compliance with Article 5(2) of the UK GDPR.	Urgent
The organisation takes accountability for ensuring all processors comply with the terms of the written contract(s)	See a.16.	See a .16.	
The organisation has a process to ensure all processing activities are documented accurately and effectively	a.17. BMBC does not currently have any robust data mapping or information audit processes in place. This means that the Record of Processing Activities (RoPA), Information Asset Registers, or	a.17. Auditors are aware BMBC is currently working to implement more comprehensive data flow mapping, as evidenced in the template provided to ICO auditors. BMBC should work to implement this new data	Medium

Governance & Accountability

Control	Non-conformity	Recommendation	Priority
	risk assessments may be incomplete or inaccurate.	mapping process to ensure that its RoPA, IARs, and risk assessments are complete and accurate reflections of their processing.	
There is an internal record of all processing activities undertaken by the organisation	a.18. BMBC does not have a central review log for their RoPA - this is managed within services. This means there is no oversight of reviews by the DPO, and no assurance that reviews are taking place regularly and consistently.	a.18. BMBC should introduce a centralised review log for the RoPA, to make sure there is oversight on the review process and that reviews are taking place regularly and consistently.	Medium
The information documented within the internal record of all processing activities is in line with the requirements set out in Article 30 of the UKGDPR	a.19. BMBC's RoPA does not include the name and contact details of the controller, a lawful basis for processing for all records, or processing carried out by processors. This means BMBC is in non-conformance with Article 30 of the UK GDPR - which designates the responsibility for controllers to maintain a RoPA and includes details on what should be recorded.	a.19. BMBC should ensure their RoPA contains all the information required by Article 30 of the UK GDPR, and details processing undertaken by processors. This will ensure that BMBC is conforming with Article 30.	Urgent
The lawful basis and condition(s) for processing personal data, special category data and data relating to criminal convictions and offences has been identified appropriately, defined and documented internally.	a.20. ICO auditors were advised that the lawful basis for processing for each activity is documented in privacy notices, and BMBC does not maintain a centralised internal log of lawful bases for processing. In cases where Legal Obligation is the basis for processing, there is no central record of what the obligation under law is for that type of processing. Where Public Task is the lawful basis for processing, there is no central record of the task or function, and the associated law or statute. Where special category data is processed, there is no central record of the additional information required to undertake this processing. This means there is no assurance that BMBC is choosing the correct basis for processing, or that BMBC is processing personal data in compliance	a.20. Implement a central log of lawful bases for processing for all processing activities - including details of any law, statute, or additional obligation for that processing. This could be incorporated into the RoPA, the APD, or in a separate document or record. This will provide assurance that BMBC is selecting the right basis for processing and is compliant with Articles (5)(1)(a) and 5(2) of the UK GDPR.	Urgent

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	with Article 5(1)(a) and 5(2) of the UK GDPR- personal data should be processed lawfully, fairly and transparently, and that controllers should be able to demonstrate their compliance with the legislation.		
There are records of when and how consent was obtained from individuals.	a.21. ICO auditors were advised that records for consent were managed within services, and there is no oversight by the DPO of how these are managed or reviewed. There is also currently no mechanism to prompt a review of consent. This means that there is no assurance that records of consent include the correct information - i.e. who gave consent, when, what was consented to, how it was given, and that it is still valid. This creates a risk that BMBC could be processing personal data in non-conformance with UK GDPR Articles 6(1)(a) and 9(2)(a), which state that processing of personal data is only lawful when the data subject has given their consent for specific purposes.	a.21. BMBC should create a central log and review schedule of consent records. This will provide oversight on how records are managed and reviewed and give assurance that BMBC is processing personal data in conformance with UK GDPR Articles 6(1)(a) and 9(2)(a).	Medium
Consents are regularly reviewed to check that the relationship, the processing and the purposes have not changed and there are processes in place to refresh consent at appropriate intervals.	See a.21. a.22.There is no assurance around consent that is given verbally as part of a new episode of care. ICO auditors were informed that there is a requirement for consent to be recorded, however there is no assurance that the conversation takes place. There is a risk that BMBC could be processing personal data in non-conformance with UK GDPR Articles 6(1)(a) and 9(2)(a).	See a.21. a.22. BMBC should consider ways it can record this type of consent more thoroughly and accurately, and methods of providing assurance around these records. This will ensure that BMBC is processing personal data in line with UK GDPR Articles 6(1)(a) and 9(2)(a).	Medium
Where the lawful basis is Legal Obligation, the organisation has clearly	See a.20.	See a.20.	

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
documented the obligation under law for that type of processing activity for transparency purposes.			
Where the lawful basis is Legitimate Interests, the organisation has conducted a legitimate interests assessment (LIA) and kept a record of it.	a.23. ICO auditors were advised that HR functions are often carried out using the lawful basis of Legitimate Interest, however no formal documented Legitimate Interests Assessment (LIA) has been carried out. This means that BMBC is processing personal information without properly assessing the balance against the interests of the controller. BMBC is also in breach of Article 5(2) of the UK GDPR, the Accountability principle.	a.23. BMBC should undertake an LIA to ensure that the interests of the controller are adequately balanced against the rights and freedoms of the data subject.	Urgent
Where the lawful basis is Public Task, the organisations is able to specify the relevant task, function or power, and identify its statutory or common law basis for processing.	See a.20.	See a.20.	
The organisations privacy information or notice includes all the information as required under Articles 13 & 14 of the UKGDPR.	a.24. It was noted while reviewing BMBC's privacy information that in order to submit a contact form - which BMBC directs users to when they wish to make an individual rights or FOI request - that allowing all cookies is mandatory in order to submit the form. By not providing additional contact details should individuals need to convey their request in writing, consent for these cookies does not meet the thresholds set by the UK GDPR. This extends to cookies across	a.24. Consider implementing a pop-up or dashboard that allows users to actively choose which cookies they consent to. Provide additional contact details such as postal address or an email address where individuals can submit their requests, so that the online form is not the only way individuals are able to contact BMBC regarding a request. This will ensure that individuals are not forced into accepting	Medium

Governance & Accountability

Control	Non-conformity	Recommendation	Priority
	BMBC's website, where consent for cookies is assumed rather than active. This is not compliant with Regulation 6 of PECR, which requires consent for cookies to meet the UK GDPR threshold - consent should be freely given, specific, and informed.	cookies they do not want to and means that BMBC will comply with Regulation 6 of PECR.	
The organisation actively publishes or communicates privacy information to keep their service users or customers informed on how their data is collected, processed and / or shared.	a.25. It was reported to ICO auditors that no privacy dashboards were offered to individuals. This means that individuals are unable to manage their privacy preferences and are not fully aware of how their personal data is being used, meaning they may not be aware of their rights or how their information is being processed.	a.25. Consider introducing a privacy dashboard, where individuals can manage their preferences, and can gain more insight into how their personal data is used - which will ensure individuals are fully informed of their rights and how their personal information is being processed.	Low
Privacy information is concise, transparent, intelligible and uses clear and plain language	a.26.A. There is currently no DPO oversight of privacy information, and it is up to individual services to create their privacy notice from a provided template. There is a distinct disparity between services as to what information is included. The lack of oversight means that they are not moderated or standardised, and they may fail to meet the requirements of the UK GDPR. B. Privacy information is not currently provided in other languages. This presents a barrier to individuals who are not fluent in English - if they cannot understand the privacy information, it has effectively not been provided.	a.26.A. BMBC should introduce a centralised log of privacy notices, in order to both maintain a historic log and to provide DPO oversight. This will provide an opportunity for the DPO to moderate and standardise what information is included, ensuring they meet the full requirements of the UK GDPR. B. Privacy information in other languages should be available to individuals, to ensure that they fully understand how their data is being processed.	Medium
Existing privacy information is regularly reviewed and, where	a.27.A. There is no review schedule for privacy information, so there is a risk that the information is out of date and individuals are not	a.27.A Introduce a review schedule for privacy information, including reviewing alongside the RoPA, to ensure that the	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
necessary, updated appropriately.	being adequately informed of how their personal data is being processed. B. BMBC does not have a log of historic privacy notices, meaning there is no assurance around what privacy information has been provided to individuals on certain dates. C. BMBC does not currently conduct user testing on its privacy information. This means BMBC has no assurance on the effectiveness of the communication of its privacy information.	information given to individuals is up to date and explains how personal data is being processed. B. See a.26.A. C. BMBC should conduct user testing on its privacy information, which will ensure that BMBC has assurance that its privacy information is effective and understood.	
Fair processing policies and privacy information are understood by all staff and there is periodic training provided to front line staff whose role includes the collection of personal data on a regular basis.	a.28. Fair processing and privacy information is not included as part of the basic GDPR training across BMBC, nor is specialised training provided to front line staff. If staff are not fully informed and trained, individuals may not be provided with the correct information, risking a breach of UK GDPR.	a.28. Fair processing and privacy information should be incorporated into basic GDPR training, and specific training should be provided to front line staff. This will make sure that the correct information is provided, and a breach of the UK GDPR does not occur.	Low
Systems, services and products have data protection 'built in' by design.	a.29.A. It was reported that BMBC do not currently use any privacy-enhancing technologies (PETs), nor are there specific system functions that are designed to protect personal data automatically. BMBC are at risk of not adequately considering the privacy rights of individuals and prioritising functionality over privacy, therefore not meeting the requirements of Article 25 of the UK GDPR which states that the controller shall "implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as	a.29.A. BMBC should consider what PETs are available to them and how they can implement PETs within their own systems, including introducing specific system functions to automatically protect personal data. They should also ensure that individuals have access to tools to find out how their personal data is being used and consider what measures can be put in place, so individuals do not have to take any specific action to protect it. This will provide assurance that BMBC are fully considering the rights of individuals and meeting the	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." B. BMBC does not currently have any tools to assist individuals in determining how their personal data is being used, nor are there any demonstrable measures in place to ensure individuals do not have to take specific action to protect their privacy. BMBC are at risk of not adequately considering the privacy rights of individuals and prioritising functionality over privacy, therefore not meeting the requirements of Article 25 of the UK GDPR.	requirements of Article 25 of the UK GDPR. B. BMBC should ensure that individuals have access to tools to find out how their personal data is being used and consider what measures can be put in place, so individuals do not have to take any specific action to protect it. This will provide assurance that BMBC are fully considering the rights of individuals and meeting the requirements of Article 25 of the UK GDPR.	
The organisation proactively takes steps to ensure that through the lifecycle of the processing activities they only process, share and store the data they need in order to provide their products or services.	a.30. There are not currently any policies in place regarding data minimisation or pseudonymisation/anonymisation, and as such data is not periodically reviewed to consider whether minimisation or pseudonymisation is appropriate. By not considering where it can reduce the amount of personal data being processed, BMBC is not compliant with Article 5(b and e) of the UK GDPR - which state that personal data should be limited to what is necessary and kept in a form that identifies individuals for longer than necessary.	a.30. Create a policy or policies documenting when and how data minimisation or pseudonymisation should occur and implement a review schedule to make sure that data is reviewed for opportunities to minimise or pseudonymise on a regular basis. This will ensure BMBC are compliant with Article 5(b and e) of the UK GDPR.	Medium
Existing policies, processes and procedures include references to DPIA requirements	a.31. BMBC have been unable to evidence any reference to DPIAs within change or project management policies. If the requirements for a DPIA are not integrated in the early stages of planning, there is a likelihood that the requirement of privacy by design and default will	a.31. BMBC should ensure that DPIA requirements are detailed in all change or project management policies. This will ensure DPIAs are considered in the earliest stages of a project, and that privacy by design and default is integrated from the	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	not be met, and BMBC is at risk of non-conformance with Article 35 of the UK GDPR - "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."	start - ensuring they conform with the requirements of Article 35 of the UK GDPR.	
The organisation understands the types of processing that requires a DPIA and uses a screening checklist to identify the need for a DPIA, where necessary.	a.32.A. Evidence provided to ICO auditors of BMBC's DPIA template showed that the template does not refer to the most current legislation. This means that BMBC's DPIA process is unlikely to meet the standards required by the UK GDPR, and there is a risk that a DPIA is not carried out when it should be. B. BMBC do not keep records of occasions where, following completion of the DPIA screening checklist, the decision is made not to undertake a full DPIA. This means the rights and freedoms of individuals may not be taken into account, and there is a risk of non-compliance with Article 35 of the UK GDPR.	a.32.A. BMBC should update their DPIA template to incorporate the requirements of the UK GDPR. This will ensure that their process is compliant with the most up-to-date legislation. B. BMBC should start documenting the decision not to undertake a DPIA. This will ensure that reasons are evidenced and considered fully, minimising risk of infringing the rights and freedoms of individuals and non-compliance with Article 35 of the UK GDPR.	High
The organisation has created and documented a DPIA process	a.33. BMBC has been unable to evidence a documented DPIA policy or procedure. The Privacy Impact Assessment Guidance provided has not been updated since the introduction of the UK GDPR and DPA18, and there is a likelihood that the DPIA process may not sufficiently meet the requirements of Article 35 or 39 of the UK GDPR.	a.33. Create a documented DPIA policy or procedure, updated to include the requirements of the UK GDPR and DPA18. This gives assurance that the process meets the requirements of Articles 35 and 39 of the UK GDPR.	High

Governance & Accountability

Control	Non-conformity	Recommendation	Priority
DPIAs are undertaken before carrying out types of processing likely to result in high risk to individuals' rights and freedoms and meet the requirements as set out in Article 35 of the UKGDPR.	a.34. There is minimal oversight of DPIAs by the DPO, and there is no set requirement to consult them during the DPIA process. There is a risk that Article 35(2) of the UK GDPR - "The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment" - is not met.	a.34. DPIAs should be overseen by the DPO and contain an area to record their advice and recommendations. The DPIA policy or procedure should reference the requirement to consult the DPO for advice during the process. This will ensure that Article 35(2) is met.	High
The organisation acts on the outputs of a DPIA to effectively mitigate or manage any risks identified.	a.35. There are no set parameters for when a DPIA needs reviewing, and the DPO does not have any oversight of DPIA reviews. This creates a risk of BMBC being in breach of the UK GDPR as they are not sufficiently mitigating the risks of processing.	a.35. The DPIA policy or procedure should detail when a DPIA needs reviewing, e.g. on an annual basis or when a parameter of processing changes. The DPO should have regular oversight of DPIA reviews to ensure they are being completed correctly. This will ensure BMBC is adequately mitigating the risks of processing in compliance with the UK GDPR.	High
The organisation has implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively	a.36.A. The Personal Data Breach Reporting Policy and Procedure is out of date, and as such refers to the DPA98 rather than UK GDPR or DPA18. There is a significant risk that the policy does not accurately reflect BMBC's obligations under the newer legislations, such as the threshold for reporting a data breach and what information needs to be included in a report to the ICO. B. BMBC does not have specific training in place to ensure staff recognise a personal data breach or near miss, so there cannot be assurance that they are recording, reporting, and preventing data breaches correctly. This could result in a breach of Article 33 of the UK GDPR, which says "in the case of a personal data breach, the	a.36.A. BMBC should update their Personal Data Breach Reporting Policy and Procedure to include the UK GDPR and DPA18, and the obligations they place on controllers regarding personal data breaches. This will ensure that BMBC has a clear, consistent approach to data breaches and can fulfil their obligations under Article 33 and 34 of the UK GDPR. B. Formulate a specific training module around data breaches and near misses. By ensuring staff have appropriate training around recognising, reporting, and preventing data breaches, BMBC will have ongoing assurance that they are maintaining compliance with Articles 33 and 34 of the UK	Urgent

Governance & Accountability

Control	Non-conformity	Recommendation	Priority
	controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority", and/or Article 34 of the UK GDPR - "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay." C. BMBC's Personal Data Breach Log does not include near misses at present, nor does it include details on the effects of the breach or any remedial action taken. The absence of specific training or a documented procedure means near misses are unlikely to be recognised and reported. This means BMBC is unable to ensure that they are adequately documenting data breaches. Where specific details such as effects or remedial action are not included, it means that BMBC are unable to carry out any analysis on individual incidents or trend analysis more broadly. As such, measures cannot be taken to prevent the same incident recurring, or to identify and remedy themes or trends.	GPDR. C. Create an area for recording near misses, effects of the breach, and remedial action taken on the Personal Data Breach Log. This will ensure that BMBC are recording breaches and near misses appropriately and can conduct analysis on both an individual and broad scale to inform mitigating and remedial actions.	
There are mechanisms in place to assess and then report relevant breaches to the ICO (within the statutory timeframe) where the individual is likely to suffer some form of damage e.g. through	a.37.A BMBC does not have a formal, documented process in place for considering whether to report a data breach to the ICO, meaning there is a risk the correct decision may not be made. If BMBC fails to report a breach that should have been reported, it would be in breach of Article 33 of the UK GDPR.	a.37.A. See b.31. B. BMBC should update their Personal Data Breach Log to include an area for recording whether a breach has been reported and details of the decision-making process. This would ensure that they are in compliance with Article 33(5) of the UK GDPR.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
identity theft or confidentiality breach.	B. BMBC's Personal Data Breach Log does not include an area to record if a breach has been reported and the reasoning behind the decision. This means that in the event the breach was required to be reported, BMBC is unable to evidence the reasoning for the decision to not report. This means BMBC could breach Article 33(5) of the UK GDPR, which states "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."		
There are mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms	a.38.A. BMBC does not have a formal, documented process in place to inform affected individuals about a data breach that is likely to result in high risk to their rights or freedoms. This means that BMBC may fail to properly notify an individual, resulting in a breach of Article 34(1) of the UK GDPR. B. There is no oversight by the DPO of responses to individuals involved in a data breach, meaning there is little assurance that the response is compliant with Article 34(2) of the UK GDPR, which states that "The communication to the data subject...shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)".	a.38.A. Create a formal process for responding to individuals involved in a data breach, including when individuals need to be notified and what information needs to be incorporated in the communication to them. This will ensure that BMBC can demonstrate its compliance with Article 34 of the UK GDPR. B. Include the requirement to have sign-off from the DPO before sending out a notification to an individual. Alternatively, consider creating a standard template for notifying individuals that is DPO-approved, to ensure that the correct information is included and BMBC is complying with its obligations under Article 34 of the UK GDPR.	High

Information Security

Control	Non-conformity	Recommendation	Priority
There is an Information Security Policy in place, which is approved by management, published, communicated to employees and subject to regular review.	b.1. There is an Information Security (IS) Policy in place which covers the main expected topics. However there is a lack of version control or summary table. It was not clear when this policy was last reviewed. Key elements of the policy are communicated to staff via the Personal Commitment Statement which they must confirm they have read and understood. If policies are not version controlled and regularly reviewed there is a risk that policies may not reflect current practice, latest sector guidance or legal guidance. Lack of evidence and review means that BMBC cannot demonstrate that it is acting in line with its legal responsibilities under UK GDPR Article 5.2 ('Accountability Principle') and UK GDPR Article 24.1 which says that controllers should have appropriate technical and organisational measures in place and that these should be 'reviewed and updated where necessary'.	b.1.Ensure that all policies have version control and summary tables in place to record details such as owner, date of review and updates to the policy. This will help BMBC meet its obligations under UK GDPR Articles 5.2 and 24.1. See also a.7.	High
Information security is incorporated within a formal training programme	b.2. There is mandatory GDPR eLearning in place for all staff. The training includes key elements of IS and has a quiz at the end with a set minimum pass rate of 80%. The training was designed by the Association of Greater Manchester Authorities in 2018. It is not clear whether the content has been reviewed or updated since.	b.2. The content of the GDPR training should be reviewed and where necessary updated or if this isn't possible additional training should be rolled out to staff to cover any gaps in the GDPR module. When reviewing eLearning content, consideration should be given to the latest threat, sector guidance and trend analysis of the BMBC data breach log to understand which key topics should be covered. The National Cyber Security Centre has produced some training for Cyber Security which may be useful to gain an understanding	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
		of which key topics should be covered for cyber threats. See NCSC Cyber Security Training.	
Lead responsibility for the strategic direction and oversight of IS has been assigned to an executive board member (e.g. Chief Information Officer or IT Director).	b.3. Staff interviewed demonstrated an understanding of their roles and responsibilities. However, this wasn't always clearly recorded within key documentation. Overall IG responsibilities have been documented in the IG Framework. However, not all roles with responsibilities specific to IS have been documented in IS Policy. For example the Chief Information Officer (CIO), the Senior Information Risk Owner (SIRO) and the Data Protection Officer (DPO). Some roles with operational responsibilities have been documented within the IS Policy, however there is no reference to the role of Buildings/ Facilities Management, the Operations Safety & Resilience Manager, Information Asset Owners (IAOs) and Information Asset Administrators (IAAs). If roles are not correctly documented and understood by key staff, there is the risk of responsibility drift and a lack of long term strategic focus and direction. This could lead to a lack of a central compliance culture across the council and ultimately non-compliance with IG legislation.	b.3. Review the IS Policy to ensure all staff with strategic and operational responsibilities for IS are included. Alternatively the roles and responsibilities within the IG Framework could be expanded to include clear IS roles and responsibilities. The IS Policy could then refer back to the IG Framework for further detail. See also a.7.	Medium
Operational responsibility has been assigned for the development and the	See b.3.	see b.3.	

Information Security

Control	Non-conformity	Recommendation	Priority
implementation of information security within the organisation.			
A steering group meets regularly to mandate, and monitor IS improvements.	b.4.A. There are several groups which consider IG and IS matters. There is an IG Group which is chaired by the SIRO and attended by the DPO and CIO. The SIRO has responsibilities for Core Corporate Services and has good oversight of these areas. The Caldicott Guardians for Children's Services and Adult Services also attend. It is possible other service areas may not have the same input or be able to feedback to the same extent on IG matters. If services are not able to feedback on these issues, there is a risk BMBC will lack central oversight of issues and risks across the organisation. There is also a risk that service areas may take divergent or non standardised approaches to promoting IG policies and compliance. B. There is also the IT & Digital Weekly Operations Board which is attended by key IT staff including the Head of ICT and the Information Security Manager and the ICT Unit Management Team which meets monthly and is attended by key staff from operational areas. The IS Policy appears to be outdated and refers to an ICT Security Working Party. C. There appears to be no documented or oversight link between the IT Governance groups and the IG Group. However the CIO who has responsibility for IT security does sit	b.4. A. BMBC should consider either adding representatives from other key services areas to the IG Group or creating an IG Steering Group which sits under and reports into the IG Group with key representatives from all services areas of the Council. This will help to ensure that overview of IG risks is more rounded and help to embed a more centralised version of compliance across the council. B. Update the IS Policy to refer to the IT & Digital Weekly Operations Board and the ICT Unit Management Team Meetings C. Ensure that either the minutes from the IT & Digital Weekly Operations Board and the ICT Unit Management Team Meetings are made available to members of the IG Group or the CIO should consider giving a summarised update of key issues/ concerns from these groups at each IG Group meeting. This will ensure a connection between IG and ICT security is maintained and fully documented. D. BMBC should ensure that IAOs and IAAs carry out periodic checks on the security of personal data once staff are allowed to work on a more regular basis within the Council buildings. The checks could include security	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	on the IG Group. If there is no clear governance link between these groups, then there is a risk of a disconnected approach to governance and oversight of IG and ICT security issues. This could lead to duality or divergence in how compliance with IS should be managed. D. It wasn't clear to what extent physical security of personal data was considered by these groups as a standing agenda item. It is likely that physical security will be discussed as a side product of records management and compliance with information security standards such as PSN and the Data Security & Protection Assessment Toolkit. Security walk arounds were carried out as part of the GDPR internal audit. However, there is no regular reporting around standard information security compliance checks.	walk arounds to check storage areas are locked, that desks are clear, and screen are locked when staff are away from desks and that documents are not left lying around at printers or in other areas. Results should be recorded and feedback back to staff involved and the IG Group.	
There are appropriate security controls in place for home or remote working.	b.5. It was reported that Remote Working and Home Working requirements were assessed as part of the Covid - 19 contingency plans asking staff to work from home. The Remote Working Policy says it was last reviewed in 2013. It was not clear when the Individual Homeworking Policy was last reviewed or updated as it didn't include version control or a summary table. If version control information is not updated BMBC will not be able to evidence that it has reviewed its technical and organisational measures to ensure they remain adequate and in line with UK GDPR Article 24.1.	b.5. Update the Remote Working Policy to include up to date version control information and the date of review. The Individual Homeworking Policy should be updated to include version control and a summary table to detail any reviews of updates. This will help BMBC to evidence its reviews of these security arrangements.	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
Hardware and software assets have been identified, documented and classified; and appropriate protection responsibilities have been defined.	b.6.ICO auditors were provided with evidence of centralised asset management for hardware & devices, servers and applications. The IS Policy references asset registers held by a nominated officer in each service area. It wasn't clear to what extent service areas would hold and manage local hardware registers now that the most staff have an assigned a Multimedia Device (laptop or tablet) via IT and a log of these is maintained on Support Works by the Service Desk.	b.6. Review and update the IS Policy to ensure that it reflects current practice with regards to the management of IT hardware and software assets.	Low
Hardware and software asset registers/inventories are subject to periodic risk assessment	b.7. There is no formally documented risk assessment methodology within the IS Policy around assessment of risks to hardware and software assets. The Applications Inventory includes a risk status based on the importance of the application to core services. However, there doesn't seem to have been a risk assessment documented for IT hardware and server assets. If risks to assets which store or process personal data have not been assessed this may be in breach of UK GDPR Article 5.1.(f) 'Integrity and confidentiality principle'. Also UK GDPR Article 32.1 says there should be a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures. It is also important to review these measures as the context of the organisation changes, the risks applied to different assets may alter in severity or likelihood, and controls may become outdated.	b.7. Create and document a risk assessment methodology within the IS Policy for assessing IT hardware (including servers) and software assets. Assessments could include the owner of the asset, location, a risk assessment based on the criticality of the asset to the organisation, security category and estimated value, any key threats and vulnerabilities, likelihood and impact, existing controls and gap analysis. A generic assessment may be applicable for some assets and should be referenced. These risk assessments should be revisited periodically to check whether the threat status has changed.	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
There are procedures in place to ensure all employees (permanent and temporary staff) and third party users return all hardware assets upon termination of their employment, contract or agreement.	b.8. Evidence was provided to ICO auditors on the return of IT hardware/ assets when a member of staff leaves BMBC. However, the IS Policy doesn't document the process. If processes aren't adequately documented, there is a risk that BMBC cannot demonstrate it has appropriate polices in place for the management of its devices/hardware. There is also the risk that different staff or service areas may diverge from the expected processes to varying degrees.	b.8. Update the IS Policy to include details of the process for allocation and return of IT assets.	Low
There is a documented governance structure surrounding the use of removable media.	b.9. It was reported that BMBC may not keep an up to date list of all USB sticks. It is felt the risk is low due to the devices being encrypted. Whilst the risk of data breaches may be lower through the use of encrypted devices, a list should be maintained for audit/evidence purposes. It will also help BMBC to know which USB stick devices are in use and who has access to these. Without an up to date list BMBC may be a risk of not being able to evidence control of these devices.	b.9.Ensure that an updated list of all USB sticks provided by the BMBC is maintained.	Low
Media containing information is protected against unauthorised access, misuse or corruption during transportation.	b.10. There are documented rules in place around the transportation of data via removable media within the IS Policy, the Personal Commitment Statement and the Records Management Policy. However, no formal risk assessment has been documented around how data should be safely transported. It was reported that staff do assess the risks, but this was on an ad hoc and informal basis. If risk assessments are not clearly	b10. Document a formal risk assessment around methods of transporting removable media. These assessments should be periodically reviewed.	Low

Information Security

Control	Non-conformity	Recommendation	Priority
	documented and reviewed periodically there is a risk that BMBC may not be able to evidence that sufficient consideration was given to the risks involved in transportation of certain times of removable media in compliance with UK GDPR Article 32.1 which says that measures in place should be assessed and reviewed to ensure they remain sufficient.		
There are endpoint (port) controls in place to prevent unauthorised use of removeable media or the upload or download of unauthorised information.	b.11.There are currently no endpoint controls in place to prevent unauthorised use of removable media. If there is no endpoint control, the organisation risks that personal data may be removed from its systems or systems may be compromised. It may also be in breach of UK GDPR Articles 24 and 32 which says that appropriate technical and organisational measures should be in place.	b.11. BMBC should consider adopting Group Policy controls to manage access to endpoint devices. This will allow BMBC to select which devices are able to use endpoints/ ports.	High
Removeable media is disposed of securely when no longer required, using formal procedures.	b.12.Devices and hardware are securely disposed of. However, BMBC don't receive a certificate of destruction from their third party disposal service provider. This means that BMBC is unable to evidence secure destruction of hardware and devices or be able trace destruction for audit and investigation purposes.	b.12.Ensure that a receipt of certificate of destruction is obtained from the third party disposal service provider. This should record the date, either list or provide detail of the weight or number of devices taken, method of destruction and date of destruction. This is normally signed off by an appropriate person from the supplier. BMBC should keep the receipt or destruction certificate for audit purposes. Certificates or receipts can be disposed of in line with the corporate retention schedule.	Medium
Appropriate background checks are carried out on personnel (employees, contractors, and third-party users) if required for	b.13.The requirements for some staff roles to undertake security clearance checks prior to commencement of employment is not referenced within the ICT Access Control Policy or Records Management Policy.	b.13. Ensure requirements around security clearance checks for certain staff roles and access to certain systems is reflected in the Access Control Policy and Records Management Policy.	Low

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
their duties and responsibilities.	The practice of undertaking security checks on some staff roles should be referenced within key IS policies to evidence that consideration has been given to these requirements in line with UK GDPR Articles 5.1.(f) ' Integrity and confidentiality principle' and 32 'Security of processing'.		
The allocation and use of privileged access rights is restricted and controlled.	b.14.Interviewees described that the process for allocation of and removal of privileged access rights. However, the ICT Access Policy doesn't reference this process. It also isn't clear whether service areas have a documented process for management of privilege access rights for their service specific applications. Without a formally documented process, there is the risk that access rights will be granted in an inconsistent or incorrect fashion, and that poor records will be kept.	b.14. Ensure that a documented process is in place around the granting and removal of privileged access rights for both central IT systems and applications managed at service level.	Medium
User access rights are reviewed at regular intervals	b.15. No formal regular reviews of user access rights have been carried out. System owners may request sight of users with access to systems on an ad hoc basis. If users change role and retain all their previous rights, they may keep access to personal data which is no longer relevant to their job role. Retention of key system access rights should be caught partially by the internal movers process which is managed by the IT Service Desk. However this may not capture access rights to service	b.15. BMBC should carry out regular sample checks of staff access rights on key systems to check that staff have the correct access based on their role. The results of any checks should be recorded and reported back to the relevant service area and governance groups. This will help to provide assurance that access management processes are working as expected.	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	specific applications. Further, if the context of a role has changed, those staff may no longer require the same level of access previously needed. This may lead to a breach of UK GDPR Article 5.1(f)'Integrity and confidentiality' principle.		
Access rights are restricted or removed in a timely fashion for all staff	b.16.Interviewees were able to describe how movers and leavers access rights were granted, altered or removed. However, no formally documented IT movers and leavers process was provided as evidence. If processes are not formally documented there is a risk that BMBC cannot demonstrate that it has appropriate technical and organisational controls in place to govern access to systems which hold and process personal data. There is also the possibility that practices may diverge between expected practice and reality and may be applied differently between service areas.	b.16.Document the movers and leavers process for altering and removing access rights to systems and applications.	Medium
Access rights are adjusted upon a change of assignment/role	see b.16.	see b.16.	
Secure areas (areas that contain either sensitive or critical information) are protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	b.17. All staff are provided with electronic card passes to access non public areas of the main council buildings and workspaces. Further security such as fobs and pin code access are required to access more sensitive areas. The IS Policy contains some details around physical security and access controls. However, these seem to be focused on access to the Computer Suite rather than general building access controls. UK GDPR Article 5.2	b.17. Either expand on physical access controls for buildings within the IS Policy or create a separate physical access policy which sets out all the access controls measures in place around BMBC's offices and buildings where personal data or It systems may be accessed.	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	requires the controller to evidence compliance with the principles set out in Article 5.1(f) Integrity and confidentiality Principle. As the IS Policy doesn't clearly document these requirements BMBC are at risk of non compliance.		
Regular risk assessments and testing are undertaken to provide assurances that effective physical security controls are in place	b.18.A. In the past, the SIRO has carried out an ad hoc security walk-around and clear screen and desk check within the Town Hall. Internal Audit also conducted an after hours walk around to check on security of devices and information in Town Hall and 3 Knowsley Place. There was no evidence that IAOs and IAAs were undertaking similar periodic checks at service level. B. No evidence of formal risk assessments around physical security of IT equipment and information storage areas has been provided. The majority of staff are currently homeworking. Regular risk assessment and security testing should be undertaken and reviewed to ensure that effective physical security controls are in place. UK GDPR Article 32 states that security measures should be reviewed to test their effectiveness.	b.18.A. Whilst we recognise most staff are currently working from home, once staff return to working in BMBC's buildings, an improved schedule of regular security checks to include those at service level should be created, carried out, results documented and should also include checks done at service level by IAOs or IAAs. Other tests could also include testing of tailgating and whether staff ask for ID for an unknown person. Results should be recorded and reported back to relevant staff and the IG Group. B. A formal risk assessment should be documented for all key BMBC buildings and should include what security measures are in place and provide a gap analysis for any risks which have not been mitigated. This should be reviewed on a periodic basis or when changes occur to the layout or the use within the building.	Medium
Granting of entry / access rights is controlled, and those rights are reviewed on a regular basis to ensure that only	b.19.A. It was reported that a record of all staff with access to BMBC buildings via the electronic card is maintained. It was not clear whether access rights are ever reviewed or audited.	b.19. A & B. Document a procedure around the granting and revoking of physical access to BMBC offices and buildings. A regular sample check should be conducted to ensure that staff have the correct access permissions.	High

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
authorised personnel are allowed access	B. There is some information around buildings security which is available to staff on the intranet. This is more in the form of guidance to staff on how to apply for an access card rather than a formal Physical Access Policy. If Physical Access Controls have not been formally been documented there is a risk that BMBC cannot demonstrate it have effective organisational controls and measures in place around the protection and security of personal data. If physical access rights and processes are not reviewed on a regular basis there is no reassurance that access to restricted information is not retained by staff who should no longer have access to it.		
Manual records are stored securely and access to them is controlled.	b.20. It was reported that some staff in the Town Hall may not have access to a key safe. Keys were hidden away within a container within a drawer. If keys are not stored safely and securely there is a risk that they could be lost or stolen and access to information impeded or accessed without authorisation.	b20.Consider installing key safes for all key office areas. This will allow central and safe storage of keys to lockers and secure storage areas.	Medium
A clear desk policy is in operation across the organisation where personal data is processed.	b.21.There are clear desk and screen requirements in place. However no regular for checks are carried out.	see b.18.A.	
There is a 'clear screen' policy in operation across the organisation where personal data is processed.	See b.21. b.22.The IS Policy says that screens auto lock after 30 minutes of inactivity. This means that	See b.21. b.22.BMBC should explore the possibility of ensuring auto screen lock is engaged after a	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	if someone forgets to lock their screen and leaves their desk there is a risk that someone main gain unauthorised access to the staff members' laptop, emails and applications.	shorter period of inactivity. This will help to reduce the risk of authorised access to staff members' devices, emails and applications.	
There are records showing secure disposal of equipment (e.g. destruction logs and certificates)	see b.12.	see b.12.	
Logging and monitoring is in place to record events and generate evidence.	b.23. There is no event logging policy in place. The need for event logging is only briefly referenced within the IS Policy. This means BMBC hasn't set out its formal approach to event logging and its responsibilities in line with UK GDPR Article 32. Policies help to evidence compliance with the legislation.	b.23.Include a policy covering event logging within the IS Policy. This should set out what elements should be logged at a minimum and how these logs should be stored and when they should be consulted.	Low
The organisation has an awareness of the lifespan of current operating systems and software and has taken appropriate measures to mitigate any risks	b.24. The Software Applications Register doesn't record whether applications are approaching end of life status. Systems which are outside of their support lifespan are vulnerable to cyberattack, as they are no longer updated when new vulnerabilities are discovered.	b.24.BMBC need to keep an up to date list of any applications near end of life status so it is aware of any threats or issues this may pose and take appropriate measures to mitigate this risk.	Medium
Networks undergo regular vulnerability scanning	b.25. It was reported that any vulnerabilities detected via Nessus, McAfee and OCS would be discussed at IMT and the IT & Digital Operations Board meetings. However there is no documented process explaining how vulnerabilities detected are managed and risk assessed. If procedures are not documented, then BMBC may not be able to evidence how it manages	b.25.Document how any vulnerabilities detected are managed, risk assessed and mitigated. This should be included in the IS Policy.	Low

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	security threats in line with its responsibilities under UK GDPR Article 32.		
Patch management practices are established and effective	b.26. ICO auditors have seen evidence of patch management processes. However this has not been documented in the IS policy. Patch management processes should be documented for evidential purposes to demonstrate that BMBC has given consideration to its compliance responsibilities under UK GDPR Article 32.	b.26. Document BMBC's approach to patch management within the IS Policy.	Low
The installation of new software is controlled, and risk assessed	See b.27.	see b.27.	0
DPIAs have been carried out to understand and mitigate risks prior to IT suppliers being granted access to the organisation's assets	b.27.A. A copy of the Standard Procurement Pre Qualification Questionnaire was provided. It contained some standard security questions, particularly around previous experience. However the questions could have been expanded on to check basic UK GDPR and information security requirements. Checks should be made to ensure that risks associated with IT suppliers have been foreseen and controlled. B. A copy of the Privacy Impact Assessment (PIA) Guidance was provided. This appears to be outdated and refers to the DPA 98. The guidance doesn't reference the fact that the ICO need to be notified where risks cannot be mitigated. A PIA form was provided alongside	b.27.A. BMBC should expand their Pre Qualification Questionnaire to include more questions around GDPR and IS compliance. For example check if suppliers adhere to any recognised standards, For example ISO27001. BMBC could also ask for copies of DP Policies and IS Policies for details of what security measures suppliers have in place and what IG training staff have received. This should help to provide a baseline check of the suppliers security measures. More detailed and tailored questions should be asked where the processing may involve special category data, large amounts of personal data or where the type of processing may produce risks to security, rights and freedoms of individuals. B. See a.32.A & a.33. and a.34. Ensure there is an area of the form to also record guidance from IT where appropriate. See our guidance on DPIAs	Medium

Information Security			
Control	**Non-conformity**	**Recommendation**	**Priority**
	the guidance. The form doesn't seem include an area to record DPO and IT staff comments. If the DPIA doesn't meet the requirements set out under UK GDPR Article 35 then BMBC is at risk of non compliance.		
Contracts and agreements are in place with IT suppliers, and include relevant information security requirements	b.28. The iTrent Contract was submitted as evidence to ICO auditors. The contract is governed under the G-Cloud framework. However, there didn't seem to be any reference in the contract to reporting of information security or personal data breaches. If information security and personal data breach reporting processes are not clearly outlined in the contract there is a risk that breaches may not be reported within statuary timescales. This may lead to non compliance with UK GDPR Article 33.	b.28.Gain assurance from the supplier that it will notify BMBC within a reasonable timeframe of any information security breached or personal data breaches. All breaches should be notified to a nominated person.	High
There are processes in place to ensure that information security incidents are internally reported, assessed, classified, recorded, and analysed as quickly as possible	b.29.The Personal Data Breach Reporting Guidance doesn’t reference how personal data breaches should be investigated, escalated and risk assessed. No risk scoring matrix has been included in the guidance. If there are no clear processes in place, the organisation may not effectively respond to incidents, creating greater risks to personal data in the process.	b.29. Update the Personal Data Breach Reporting Guidance document to include reference to how personal data breaches are investigated, risk assessed and escalated. A risk matrix should be included to explain how risks should be measured.	Medium
There is an incident log in place to capture all reported incidents and near misses	b.30.The data breach log doesn't include any details of a risk assessment of the incidents, categorisation of incidents or lessons learned and whether the ICO and individuals have been notified. This means BMBC may not be able to pull	b.30. BMBC should record the information detailed opposite and carry out trend analysis reports. Reports should be provided to the IG Group. See also a.37. b.	Medium

Information Security

Control	Non-conformity	Recommendation	Priority
	trend analysis and compliance information around its performance on personal data breach reporting process and incidents.		
There are processes in place to ensure incidents are reported to the ICO as appropriate and within the required statutory timeframes (72 hrs) under the UKGDPR	b.31. There is nothing referenced within the Personal Data Breach Reporting Guidance around when BMBC are required to report incidents to the ICO and what information needs to be provided. If the process is not clearly documented BMBC may not report incidents when required and may be at risk of non compliance with UK GDPR Article 33.	b.31. Update the Personal Data Breach Reporting Guidance document to refer to the fact that the ICO needs to be notified within 72 hours of BMBC becoming aware of an incident and where the breach is likely to result in a risk to the rights and freedoms of individuals. It should also set out the information that needs to be provided to the ICO as part of the notification process (see UK GDPR Article 33.3)	High
There are mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms	b.32. Some guidance is provided within the Personal Data Breach Reporting Guidance about notifying individuals of a personal data breach. However, there is no reference to the threshold under UK GDPR Article 34.1 which says that if a personal data breach is likely to result in a high risk to the rights and freedoms of individuals then they should be notified. If this requirement isn't documented, then BMBC is at risk of not complying with this requirement as staff may not realise when individuals have to be notified (and when it is not just discretionary).	b.32.Update the Personal Data Breach Reporting Guidance document to include reference to the need to notify individuals when the risk is likely to result in a high risk to the rights and freedoms of the individual. See also a38.A.	Medium

Freedom of Information

Control measure	Non-conformity	Recommendation	Priority
Policies and procedures are in place which explain the organisation's approach to, and responsibilities for, FOI and EIR regulations	c.1.A. Whilst FOI policies and procedures are in place the documents are out of date and need updating to reflect current BMBC practice. B. Not all policy and procedure documents have owners and are not adequately controlled. This may lead to staff following incorrect or using out of date policies and procedures.	c.1.A. BMBC should review and update its current policy and procedure documents for FOI so as to provide an accurate and cohesive range of documents for staff use. B. BMBC should apply comprehensive document controls to its published policies and procedures and then review those documents on a regular basis.	Medium
Policies and procedures are easily accessible by staff	c.2. No explicit provision has been made to make policies and procedures easily accessible to staff who do not use computers. This may result in them taking non-compliant actions on behalf of BMBC.	c.2. BMBC should make provision to ensure staff who do not use computers are aware of how they can access FOI procedures. Managers should make staff aware they can request a hard copy or can make provision for them to use the BMBC intranet.	Medium
The organisation ensures that staff are informed of any changes to policies and procedures regarding FOI/EIR regulations	c.3. Whilst updates to policies and procedures are cascaded by managers, there is no assurance that staff have read and understood them. This means that staff, particularly those who process requests in different delivery service areas may not be following current guidance and risk non-compliance with FOI/EIR legislation.	c.3. BMBC should gain assurance that staff have understood FOI/EIR updates to policies and procedures and will be able carry out their role in line with internal or statutory requirements.	Medium
There are procedures publicly available to direct individuals in how to request information under FOI / EIR.	c.4. The BMBC website only details using the online form or writing to the council to make an FOI request. This published guidance could prevent a request being made and lead to complaints being raised. Requestors may prefer to use email or other electronic means and could see this as potentially restricting their rights.	c.5. BMBC should review the web page to take into account current ICO guidance and the Section 45 Code of Practice for access to ensure that they maintain compliance with the legislation and can be seen to be acting in line with current guidance.	High

Freedom of Information

Control measure	Non-conformity	Recommendation	Priority
The organisation maintains a documented record of their receipt and handling of requests	c.5. BMBC has an FOI Case Management System (CMS) which is effective in managing and monitoring the statutory timescales for requests but has no functionality to easily report on exemptions used, refusals etc. This prevents the council form carrying out any trend analysis on requests for quality monitoring purposes.	c.5. When evaluating an upgrade or replacement for the current CMS BMBC should consider adding functions to enable trends to be easily identified for quality monitoring purposes as an aid to maintaining compliance.	Low
There are mechanisms to monitor the quality of responses to requests	See c.5.	See c.5.	
Exemptions/Exceptions should be applied on a case-by-case basis, by appropriately trained staff, with no evidence of the use of blanket exemptions/exceptions.	c.6. There is no universal formal training programme for staff with responsibility for dealing with FOI and EIR requests for information. If staff do not have the necessary skills to handle tasks such as applying exemptions and redactions, BMBC may find itself acting without compliance, and/or responding to requests in an inconsistent manner. In addition this training should be regularly refreshed to ensure the quality of responses continue to maintain compliance.	c.6. BMBC should formalise a training programme for all staff with responsibility for handling FOI/EIR requests. The training should be recorded within the staff training system. Regular refresher training should also be implemented, which again should be recorded to give assurance.	High
There is evidence of an oversight or approval process for the use of exemptions/exceptions.	c.7. There is no program of sampling of completed requests for the purposes of quality monitoring. This prevents BMBC form having any oversight as to where issues in FOI compliance may be developing.	c.7. BMBC should instigate a sampling programme for FOI responses in order to ensure a consistent quality of response and to maintain compliance.	Medium
Redactions should be applied on a case-by-case basis, by appropriately trained staff, and records should be maintained of what has been redacted.	See c.6.	See c.6.	

Freedom of Information

Control measure	Non-conformity	Recommendation	Priority
There is evidence of an oversight or approval process for the use of redactions.	See c.7.	See c.7.	
There is an induction training programme, with input from Information Governance or equivalent, which includes general training on how FOI/EIR applies to the organisation, what they currently do to comply, and how to recognise an FOI/EIR request.	c.8. By combining FOI and DP training into one module staff appear unsure as whether they have received training in FOI. This may cause confusion for staff when working with the legislation(s) that in turn could lead to non-compliance in either DP or FOI.	c.8. To ensure staff can clearly differentiate the requirements of both types of legislation the FOI training should be developed into its own mandatory eLearning module. This FOI module should be mandatory and refreshed annually in line with the DP training.	High
Staff receive refresher training in the requirements of FOI/EIR, including, where appropriate, updates from the relevant decisions of the ICO and the Information Tribunal.	See c.8.	See c.8.	
There is specific training for staff with responsibility for handling requests for information, on FOI, EIR and Codes of Practice.	c.9. There is no universal specialised formal training programme for staff with responsibility for handling requests for information, on FOI, EIR and Codes of Practice. If staff do not have the necessary skills to handle specialist tasks, BMBC may find itself acting without compliance, and/or responding to requests in an inconsistent manner. In addition there is no formal periodic refresher training for these staff, this	c.9. BMBC should formalise a specialist training programme for all staff with responsibility for handling FOI/EIR requests. The training should be recorded within the staff training system and refreshed on a regular basis to give continued assurance.	High

Freedom of Information

Control measure	Non-conformity	Recommendation	Priority
	potentially could lead to responses that are non-compliant.		
Staff receive regular reminders of how to recognise FOI/EIR requests	c.10. BMBC does not use periodic communication methods such as newsletters or reminder emails to remind all staff of how to recognise and react to FOI/EIR requests. If staff do not recognise requests, they may not inform the contact centre the request has been submitted, which may prevent it being responded to within the statutory timescale.	c.10. BMBC should undertake a programme of periodic communications to remind staff of how to recognise and respond to FOI/EIR requests.	Medium

Observations

The tables below list observations made by ICO auditors during the course of the audit along with suggestions to assist BMBC with possible changes.

Governance & Accountability	
Control	**Observation**
Privacy information is concise, transparent, intelligible and uses clear and plain language	The Assistant Director for Children's Care and Safeguarding highlighted that his directorate were planning ahead and considering working alongside SEND provision parent groups around privacy information. They currently work with these group to coproduce policies and procedures, which has been effective, and this could be an opportunity to ensure privacy information is accessible and useful.

Information Security	
Control	**Observation**
Good information security practices are promoted across the organisation.	There is no formal information governance (IG) communication plan in place. A communication plan will help coordinate and focus on key IG topics and reminders to be rolled out across the year.
There is a policy that documents the process and supports the security measures the organisation uses to manage the risks introduced by using mobile devices.	To add an additional layer of compliance, BMBC could consider asking staff to check and state that they have certain security requirements before being allowed to work from home (once normal working practices resume). This could cover for example checks that Wi-Fi passwords have been reset, that certain security standards are in place regarding locks on doors and windows.

There are procedures in place to ensure all employees (permanent and temporary staff) and third party users return all hardware assets upon termination of their employment, contract or agreement.	BMBC should consider carrying out sample checks on historic leavers to check that all hardware has been returned. This is in line with good practice
Key systems, applications and data are backed up to protect against loss of personal data.	When normal operations are resumed, BMBC should consider scheduling periodic full systems tests of the back-up of key systems to check that back-ups can be restored as expected.
The plans are tested on a periodic basis to ensure they remain up to date and fit for purpose	Following a return to normal operations BMBC should consider implementing periodic unscheduled tests of the Business Continuity Plans.

Appendices

Appendix One – Recommendation Priority Ratings Descriptions

Urgent Priority Recommendations -

These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.

High Priority Recommendations -

These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.

Medium Priority Recommendations -

These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.

Low Priority Recommendations –

These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

Credits

ICO Team Manager – Paul Hamill
ICO Engagement Lead Auditor – Helen Oldham
ICO Lead Auditor – Amelia Walsh
ICO Lead Auditor – Ian Dale

Thanks

The ICO would like to thank Sally Lever, IG Project support and Business Support Manager, Lisa Featherstone, Deputy Director Governance and Assurance and Janet Witkowski, Head Legal Services and Data Protection Officer for their help in the audit engagement.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Bury Metropolitan Borough Council.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Bury Metropolitan Borough Council. The scope areas and controls covered by the audit have been tailored to Bury Metropolitan Borough Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.