Agenda Item No:	4
Report To:	AUDIT COMMITTEE
Date:	15 March 2016
Report Title:	DATA PROTECTION AUDIT REPORT
Report Author:	Rich Clarke

ASHFORD
BOROUGH COUNCIL

Summary:	The report sets out findings and brief of the recent audit into the controls designed and operated by the Council to ensure it meets its data protection obligations. The findings and recommendations of the report have been accepted by officers, and the report includes a completed action plan wherein officers set out plans for improvements to the service.

Key Decision:	No
Affected Wards:	All
Recommendations:	**1. The Audit Committee NOTES the findings of the Data Protection audit and makes appropriate further enquiries of officers.**
Policy Overview:	Not Applicable
Financial Implications:	Not Applicable
Risk Assessment	No
Equalities Impact Assessment	No
Other Implications:	Not Applicable
Exemptions :	
Background Papers:	Data Protection Audit Report (CG03(15-16))
Contacts:	rich.clarke@midkent.gov.uk – Tel: (01233) 330442

Report Title: Data Protection

Purpose of the Report

1. Our audit plan, approved by Members in March 2015, included an audit intended to examine the controls designed and operated by the Council to ensure it meets its obligations under the Data Protection Act 1998 and associated regulations and guidance. This report represents the conclusions of that audit.

2. Since the audit was originally undertaken the Council has undergone a broader restructure meaning the key officers at the time of the review will not, in future, have responsibility for these areas. Present at the meeting will be officers who will take on these responsibilities in future who will be able to answer Members' questions about proposed actions in response to the audit.

Background

3. We began work in October 2015 against the audit brief set out from page 15 of the Audit Report. This sought specifically to examine controls against the responsibilities given to the Council by the Data Protection Act 1998, including managing subject access requests for data and recognising, handling and reporting any breach of requirements. We concluded our work and issued the report in draft in January 2016 (delayed from an original proposal of December 2015 owing to Christmas leave and changing officers responsibilities as part of the broader restructure at the Council).

4. We received a completed action plan from officers and finalised the report on 26 February 2016. Officers accepted the findings of the report and consequently there were no substantial changes in the body of the report between draft and final versions.

5. It is also important to note, when considering the scope, that the audit was not an examination of IT systems and how the authority keeps its data safe from external threat. We have, separately, a review of IT security measures on our plan for 2016/17 (also at this Committee meeting).

Risk Assessment

6. It is important to note that the report, while less than satisfactory, is not at the 'poor' level of assurance where we would note a failing service. Rather, at 'weak' level, we are describing a service which may well have elements of good practice but is not reaching the required level consistently.

7. Some of the consistent themes identified in the report were a lack of clarity on key responsibilities and limited organisation and documentation on monitoring and reporting on breaches. The Council's restructure has meant that new officers

will be responsible for taking data protection forward and giving that clarity of ownership and procedure.

Equalities Impact Assessment

8. There are no proposals made in the report that require an equalities impact assessment.

Other Options Considered

9. Not applicable

Consultation

10. The audit findings have been discussed and agreed with both the original audit sponsor at the time the work was set out, plus those officers who will take responsibility for Data Protection in future.

Implications Assessment

11. Not Applicable

Handling

12. Not Applicable

Conclusion

13. The report presents for Member comment and enquiry the results of our work on the Council's Data Protection responsibilities.

Portfolio Holder's Views

14. The relevant Portfolio Holder for audit, Cllr Neil Shorter, is a member of the Audit Committee.

Contact: Rich Clarke Tel: (01233) 330442
Email: richard.clarke@ashford.gov.uk or rich.clarke@midkent.gov.

MID KENT AUDIT

DATA PROTECTION

FINAL AUDIT REPORT

February 2016

Assurance Rating: Weak

Audit Code	ABC-CG03(15-16)	**Service**	Communications & Technology
Senior Auditor	Claire Walker	**Head of Service**	Rob Neil
Head of Audit	Rich Clarke	**Chief Executive**	John Bunnett

ASHFORD BOROUGH COUNCIL

MAIDSTONE Borough Council

Swale BOROUGH COUNCIL

Tunbridge Wells Borough Council

MID KENT AUDIT

Summary Report

We conclude based on our audit work that Data Protection has **Weak** controls to control its risks and support its objectives. We provide the definitions of our assurance ratings at appendix II.

The council has documented policies and procedures, also allocated roles and responsibilities, however there are weaknesses as policies are not operated (the monitoring checks) as described and there are no deputy arrangements to provide formal cover in the Data Protection Officer's absence. The Data Protection function is currently subject to staff changes and consideration of future service delivery and resource arrangements.

The Data Protection Policy makes clear commitments on training provision and we found that guidance was available to staff, however training and awareness arrangements are less well established. There is no mandatory post induction refresher requirement, no formal records to evidence training for key staff (such as the Data Protection Officer) and only 58 staff evidenced as having completed the E Learning package.

Compliance with Data Protection requirements is not monitored by the council (the review processes noted in policy and job descriptions) as provided for in key documents. Interviews with various services identified some services with better understanding and application of data protection requirements (such as the Monitoring Centre and Fraud Investigations). We found that the Council's Members Allowance IT Scheme required recipients to register, however only 5/23 were registered. We found that there were no central logs to record statistics and facilitate reporting (Subject Access Requests and Breach Notifications or near misses).

Staff advised that no breaches had been reported to the Information Commissioner. Arising from the absence of an incident / referral log it was not possible to assess the number or nature of any internal referrals made. In addition, the access capability to records is limited to the Data Protection Officer as material is held in E records (personal email and e filing) rather than generic E records to enable authorised deputy access.

Areas to improve
• Policies & Procedures and associated monitoring and review arrangements [R1, R2, R6] • Reporting, roles & responsibilities and associated record keeping [R3, R4, R8, R10] • Training [R5] • Record keeping [R7, R8, R9]

Next Steps

At page 10 we describe the 10 recommendations arising from our work, and response from management. We are pleased to note management have agreed to implement the recommendations which we will follow up as they fall due in line with our usual approach and consider re-evaluating the assurance rating as the service acts to address the issues identified.

Under the procedure agreed with the Audit Committee in September 2015, if the assurance rating of the final report remains as 'weak' this report plus a completed action plan will be presented in full to Members of the Audit Committee.

We have prioritised our recommendations as below:

Priority 1 (Critical)	Priority 2 (High)	Priority 3 (Med)	Priority 4 (Low)	Advisory
0	2	6	1	1

We provide the definition of our recommendation priorities at appendix II.

Findings in Context

Our most recent audit work in this area was Data Protection Act review, November 2011. That report concluded that the controls offered a limited level of assurance. Although we have changed the way in which we report ratings, meaning the results are not directly comparable, we consider that the assurance offered by controls in the service has failed to improve since that review. The 2011 management action plan resulted in some changes (for example improvements in physical security) however some concerns are being raised again (such as the need to revise policy and procedures and data retention).

Independence

We are required by Public Sector Internal Audit Standard 1100 to act at all times with independence and objectivity. Where there are any threats, in fact or appearance, to that independence we must disclose the nature of the threat and set out how it has been managed in completing our work.

We have no matters to report in connection with this audit project.

MID KENT AUDIT

Acknowledgements

We would like to express our thanks to all those officers who assisted completion of this work, in particular Rob Neil, Head of Communications & Technology.

Audit team and contact details	Report distribution list
Head of Audit Partnership Rich Clarke (Rich.Clarke@MidKent.gov.uk) **Senior Auditor** Claire Walker (Claire.Walker@MidKent.gov.uk)	*Draft and Final Report* Rob Neil, Head of Communications & Technology Terry Mortimer, Head of Legal & Democratic Services Paul Naylor, Deputy Chief Executive **Ashford BC** *Final Report Only* John Bunnett, Chief Executive Audit Committee Members

Detailed Findings

We completed fieldwork during November 2015 to the objectives and using the tests set out in the final audit brief dated September 2015. We include the audit brief at appendix I. We again thank the service for support provided to enable efficient completion of our work. Please note that the timeline has been amended from that set out in the original brief in response to officer requests for additional time to formulate a response to the action plan in the draft report.

Objective 1: To review the appropriateness of the Council's policies and procedures relating to the Data Protection Act

Ashford BC has a documented Data Protection Policy and suite of supporting guidance and policies such as the Bring Your Own Device Policy and the Internet Acceptable Use policy. Although material has been subject to revision the passage of time means that some references (such as the ISO regime) and media developments require further update [**R1**].

Provisions for operational and organisational checks are embedded in the Data Protection Policy and the Telecommunications & Data Protection Officer's job description (dated 2001) however these checks are not undertaken in practice. The Data Protection Policy provides for regular review, audits, assessments and evaluations on the way that personal information is managed (handling and management of personal information) in particular that "performance with handling personal information is regularly assessed and evaluated". The officer advised that her role was limited to registrations and co-ordinating Subject Access Requests and that the monitoring regime described in her JD had not been applied for some years. [**R2**].

The Council is currently restructuring its Information Technology function with the loss of the Head of Communications and Technology post (the incumbent Data Protection Officer / Senior Information Risk Officer). At the time of the field work the handover arrangements had yet to be determined. Currently the senior Data Protection role has no formal procedure notes, no deputy arrangement and has sole access to key records (such as potential breach reports and investigation records), through his email account and personal e-filing [**R3**] [**R4**].

Conclusion: Policies and procedures are documented and available, however they are dated and do not reflect modern media or references. Roles and responsibilities are detailed in job descriptions but they require revision to reflect changes in operation and conduct of roles, and the associated requirements placed on them through policies and procedures. The non performance of advertised compliance checks weakens the council's ability to assess compliance with data protection requirements.

R1: Policy & Procedure	Priority 3: Medium
Update and apply policies and procedures	

R2: Organisational Monitoring & Review	Priority 3: Medium
Implement a monitoring and review regime in line with policy commitments	

R3: Roles & Responsibilities	Priority 3: Medium
Revise job descriptions and supporting arrangements (Deputy and Back Up arrangements)	

R4: Shared Access	Priority 3: Medium
Records must be accessible to a minimum of 2 authorised staff	

Objective 2: To establish and review the guidance and training available to staff, and their awareness with regards to Data Protection

Information Commissioner audits of public bodies have identified that training and awareness are key to facilitating compliance with data protection requirements. The Council has limited records to demonstrate training undertaken by key staff and the general workforce. Data Protection Act refresher training is not mandatory once induction is completed. Discussions with staff found that staff recalled receiving training as part of induction but had limited recollection of the areas covered.

The Data Protection Policy states that everyone managing and handling personal information will be "appropriately trained" and that "everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice". Training has not been delivered as described; records show that 58 staff completed e training and Outlook Calendar references indicated that key staff (the Data Protection officer) had received some training. [**R5**]. Discussions with staff identified a limited awareness of the available supporting guidance available.

Conclusion: Records and discussions with staff identified little training occurred in practice and that staff awareness was limited.

R5: Training	Priority 2: High
Implement training regime and awareness programme	

Objective 3: To ascertain whether the council is compliant with the Data Protection Act 1998 and related legislation and guidance

We conducted Interviews with staff in a range of functions to assess organisational and functional awareness of and compliance with data protection requirements. Particular elements, such as Notification, Registration, Subject Access Requests (SARs), and breach notification / handling were reviewed. Discussions with staff also identified that a number of security provisions were in place to safeguard access to data in keeping with those described in policies and procedures.

We found that the Telecommunications & Data Protection Officer had records for two Council data controller registrations; the Council itself and Electoral Registration. We noted that 5 of 23 Members in receipt of IT Allowances (claimed and paid in accordance with the Members IT Allowance Scheme) were registered as data controllers. We noted that arrangements were in progress to remind Members of scheme requirements to register so have made no recommendation as the exercise is already in hand.

We found limited records to support SARs and breach notification / handling, and no central logs of such aspects [**R7**]. SARs records were held by a number of areas, and varied in the quantity and nature of records held (proof of identification, fees paid, authority for fees waived [**R8**] and lacked copies of material released). Attempts to ascertain the total number of SARS received through fees paid or waived failed as we found that staff were unsure or inconsistent in where monies were coded and did not keep records of fees waived.

Material relating to potential breaches and related investigations could not be accessed [**R6**] as it was held in one officer's email account and personal e filing [**R4**]. Material is not accessible to at least a deputy / approved officer [**R4**]. The sample emails supplied for audit review were reliant upon officer choice (there being no log from which sample selection could be made) and those provided indicated a degree of informality in processes followed and records of investigations, and the officer confirmed that there were no formal procedures.

The Data Protection Officer is responsible for decisions on whether reports are considered to be "breaches". The sample case supplied for audit review related to an alleged breach of tenant confidentiality (where the tenant refused to accept an offer of a management move) was handled through disciplinary procedures and not treated as a breach or self referred to the Information Commissioner.

Requests for details of reports on discharge of function to Management Team resulted in supply of one report, that advising of the implications arising from the proposed new

European Directive requirements. The absence of reports does not facilitate organisational review of its compliance with Data Protection [**R10**].

The suite of policies and guidance contain instructions to staff on security and confidentiality measures such as "clear desk" and "clear screen". . Discussions with staff and examination of sample records found differences in awareness and application of data protections aspects for example the Risk Register (Health & Safety) had been subject to review and action taken to handle old records; elsewhere, in Housing Options, some case files were kept on desks and in-trays. Discussions with staff (sample services) found that records were retained for longer than necessary as staff were not aware of organisational record retention guidance [**R9**].

Conclusion: Tests found that compliance with Data Protection requirements varied between services reviewed, with some pockets of good practice (such as the Ashford Monitoring Centre and the Fraud Investigation section), but partially compliant overall. The main areas of weakness related to record retention (e.g. data kept for longer than required, data security in particular storage locations and breach handling arrangements)

R6: Breach Handling	Priority 2: High
Formalise and enhance protocols for breach handling	

R7: Centralised Records	Priority 3: Medium
Devise ands maintain central records / logs of Subject Access Requests and Breaches (potential and notifications)	

R8: Fee Handling	Priority 4: Low
Formalise fee handling and banking arrangements (Subject Access Request fees)	

R9: Record Handling	Priority 3: Medium
Review and revise arrangements for data storage and retention to ensure compliance with Data protection record retention requirements	

R10: Functional Reporting	Advisory
Implement a functional reporting process	

MID KENT AUDIT

Recommendations and Action Plan

R5: Training	Priority 2: High
Implement training regime and awareness programme Regular training would increase awareness of data protection issues and facilitate awareness of and compliance with data protection requirements	
Management Response	
There will be two strands to training and awareness – (i) on general data protection issues and responsibilities and (ii) on specific Council policies and procedures. The general training will be directed at all staff and will include an awareness campaign and e-learning. The specific training will need to be based on the data protection policies and procedures that have been updated following review. The specific training will be for the data protection "key officers" that will be identified. The intranet will also be used to make guidance available and to let staff know who to contact for further advice.	
Responsible officer: Joy Cross	**Implementation date**: April 2016

R6: Breach Handling	Priority 2: High
Formalise and enhance protocols for breach handling Formalised reporting & investigation protocols, and associated records, would ensure consistency of approach and evidence the arrangements to assess, address and action issues and record work undertaken and outcomes	
Management Response	
It is accepted that providing guidance in such instances would improve consistency and provide a framework for decision making. Following up on breaches in order to learn the reasons why they occurred will also be included in order to try and reduce the risk of them reoccurring. The new guidance will be taken forward as part of the review of policies and procedures. Appropriate training and guidance will be prepared thereafter.	
Responsible officer: Nick Clayton	**Implementation date**: June 2016 (in conjunction with recommendations 1, 2, 9, 8, and 10)

MID KENT AUDIT

R1: Policy & Procedure	Priority 3: Medium
Update and apply policies and procedures Revision (main and supporting policies & procedures) would ensure material reflects best practice and enhanced provisions of key aspects such as breach reporting and related investigations. Application of policies would assist in ensuring organisational compliance with DPA requirements.	
Management Response	
The new policies and procedures will aim to be easy to understand and practical, while highlighting risks and setting out mechanisms for reducing those risks.	
Responsible officer: Nick Clayton	**Implementation date**: June 2016 (in conjunction with recommendations 6, 2, 9, 8, and 10)

R2: Organisational Monitoring & Review	Priority 3: Medium
Implement monitoring and review regime in line with policy commitments Compliance with DPA requirements would be reviewed, assessed and monitored in practice.	
Management Response	
It is important to learn from experiences in day to day operations in order to reduce the risk of non-compliance with the Data Protection Act and to monitor if policies and procedures are operating as expected. The revised policies and procedures will set out monitoring and review arrangements, bearing that in mind.	
Responsible officer: Nick Clayton	**Implementation date**: June 2016 (in conjunction with recommendations 6, 1, 9, 8, and 10)

R3: Roles & Responsibilities	Priority 3: Medium
Revise job descriptions and supporting arrangements (Deputy and Back Up arrangements) Clarification and revision would assist in developing and formalising the new regime (handover arrangements), modernising roles, and strengthening functional back up / support arrangements	
Management Response	
This will be taken forward as part of the wider restructure of the Council as well as the revised policies and procedures.	
Responsible officer: Joy Cross – Job descriptions and identifying key workers Paul Courtine – Interim point of contact pending appointment of data protection officer	**Implementation date**: July 2016

R4: Shared Access	Priority 3: Medium
Records must be accessible to a minimum of 2 authorised staff Functional resilience as material would be available to authorised staff	
Management Response	
This will be taken forward as part of the wider restructure of the Council as well as the revised policies and procedures.	
Responsible officer: Data Protection Officer	**Implementation date**: July 2016

R7: Centralised Records	Priority 3: Medium
Devise and maintain central records / logs of Subject Access Requests and Breaches (potential and notifications) Absence of central records of cases makes it difficult to monitor caseload and resource implications (SARs & other requests)	
Management Response	
This will be taken forward as part of the wider restructure of the Council as well as the revised policies and procedures. Scoping for use of the FOI tracker as a log for subject access requests is already underway.	
Responsible officer: Paul Courtine Data Protection Officer	**Implementation date**: Until July 2016 From July 2016

R9: Record Handling	Priority 3: Medium
Review and revise arrangements for data storage and retention to ensure compliance with Data protection record retention requirements Increased awareness of data retention and storage arrangements would improve compliance with data protection requirements	
Management Response	
This will be taken forward as part of the revised policies and procedures and will be an involved process due the number of different records kept and differing requirements for retention. It should though be possible to set certain retention periods relatively soon, especially where the issue was already under consideration prior to this report (e.g. emails in the archive).	
Responsible officer: Nick Clayton	**Implementation date**: June 2016 (in conjunction with recommendations 6, 1, 2, 8, and 10)

MID KENT AUDIT

R8: Fee Handling	Priority 4: Low
Formalise fee handling and banking arrangements (Subject Access Request fees) Arrangements for waiving fees should ensure consistency of approach and appropriate authority for course of action. Monies received should be coded consistently to facilitate their identification	
Management Response	
Not requiring payment of the £10 fee results in the request not amounting to a subject access request. This can facilitate providing a reply and therefore be both in the interests of the requestor (e.g. speedier reply) and the Council (e.g. less administration). The financial consequences of foregoing the £10 fee are negligible given the low number of subject access requests in the first place. Guidance for staff on fee handling and banking will though be taken forward as part of the revised policies and procedures.	
Responsible officer: Nick Clayton	**Implementation date**: June 2016 (in conjunction with recommendations 6, 1, 2, 9, and 10)

R10: Functional Reporting	Advisory
Implement a functional reporting process A periodic report on discharge of DPA aspects would enable Management Team to assess organisational compliance and discharge their responsibilities	
Management Response	
As part of the restructure of the organisation, a new post holder with responsibility for data protection will be identified. One of their roles is likely to be reporting to Management Team on a regular basis in relation to data protection. This will include updates on issues with the organisation and elsewhere (e.g. new legislation) and statistical information (e.g. the number of subject access requests). As an additional means of raising the profile of data protection within the organisation and emphasising its importance, it is intended to designate a member of Management Team as a data protection "champion".	
Responsible officer: Nick Clayton Terry Mortimer – Data protection champion on Management Team	**Implementation date**: June 2016 (in conjunction with recommendations 6, 1, 2, 9 and 8) July 2016

MID KENT AUDIT

Appendix I: Audit Brief

About the Governance Area

Corporate governance is the system of rules, practices and processes by which the Council is directed and controlled. Broader than just financial controls, it is also concerned with how the Council maintains legal compliance and seeks to arrange its operations in order to achieve its objectives.

The Data Protection Act 1998 (DPA) governs the collection, processing, use and security of personal data, while the Information Commissioner's Office (ICO) regulates the compliance with the Act. Keeping within these responsibilities requires continuing review and compliance, including appropriate management of risks as they arise. Legal compliance is therefore a fundamental duty of the Council and is crucial to its success in achieving its strategic objectives.

The Communications & Technology Service is responsible for the provision of advice to ensure that the Council complies with its responsibilities under the various items of information legislation; Freedom of Information, Environmental Information Regulations and data protection issues.

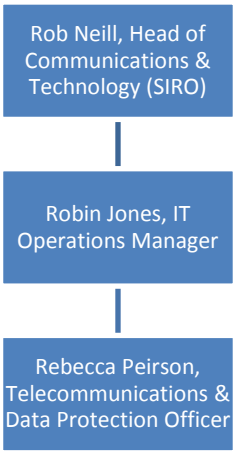
The Head of Communications & Technology (HCT) is the Senior Information Risk Owner (SIRO) and the Data Protection Officer. HCT is supported in day today practice by the Telecommunications & Data Protection Officer.

Successful management of Data Protection will help the Council to

- Ensure it remains in compliance with its legal obligations,
- Make best use of its information assets,
- Share information in line with accepted standards for common benefit.

MID KENT AUDIT

Service Structure Chart



About the Audit

The Data Protection Act (DPA) governs the collection, retention and use of personal data and is supported by a number of other regulations, Codes of Practice and guidance. From April 2010 the Information Commissioners' Office (ICO) were given powers to impose financial penalties of up to £500k for serious breaches in DPA legislation.

The audit primarily seeks to establish the Councils' compliance with the statutory requirements of the Data Protection Act, relevant legislation and guidance.

The previous audit in 2011-12 gave a Limited level of assurance. The main findings included a need for improved handling of subject access requests, promotion of the DPA throughout the council, and strengthening of physical security arrangements.

Audit Objectives

1. To review the appropriateness of the Council's policies and procedures relating to the Data Protection Act
2. To establish and review the guidance and training available to staff, and their awareness with regards to Data Protection
3. To ascertain whether the council is compliant with the Data Protection Act 1998 and related legislation and guidance

Audit Scope[1]

In order to establish compliance with the requirements of the Act, the audit will consider the following areas:

1. Data protection legislation and guidance
2. Data protection policy and procedures
3. Data protection training
4. Obtaining, processing and update of personal data
5. Disclosures (request handling processes, application of exemptions, and associated records)
6. Retention of personal data
7. Organisational security of data / breach protocols
8. Transfer and sharing of personal data
9. Arrangements with contractors / third parties
10. Management of data

Audit Testing

1. Review the Council's Data Protection Policy and other relevant guidance
2. Conduct interviews with key officers to establish and document the roles and responsibilities for data protection & establish their awareness of and compliance with data protection principles
3. Review the data protection training and guidance provided to officers & members
4. Review, for a sample of service areas, whether there is clarity around why data is being collected and how it will be processed fairly and lawfully
5. Test a sample of subject access requests received since January 2015 & ascertain whether these requests were processed appropriately
6. Review, for a sample of service areas, whether personal data is kept and shared in accordance with the DPA principles (adequate, relevant, not excessive, accurate, kept up to date, not kept longer than necessary, used for purposes for which it was obtained / consent given or relevant legal exemption applied)
7. Review the measures taken against unlawful or unauthorised processing an accidental loss, destruction or damage of data

[1] This scope is current as at the date of the document. In the event that our testing identifies further areas of audit interest we may modify/extend testing but will discuss modifications with you before undertaking additional work.

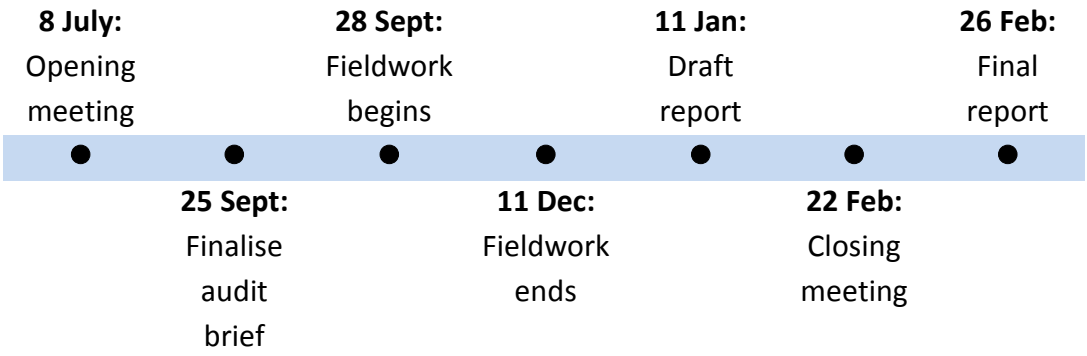
MID KENT AUDIT

Audit Resources

Based on the objectives, scope and testing identified we expect this review will require **15 days** of audit resources, broadly divided as follows:

Audit Task	Audit Resource	Number of Days (Projected)
Planning	Claire Walker	3.5
Fieldwork	Claire Walker	7.5
Reporting	Claire Walker	2.5
Supervision & Review	Rich Clarke	1.5
Total		**15**

Audit Timeline (Revised December 2015)



Council Resources required by audit

Key Contacts	
Rob Neil	Head of Communications & Technology
Rebecca Pierson	Telecommunications & Data protection Officer

Documents required	
Subject Access Reports	Data Subject Requests
Training Records	Policies, Guidance & Procedures
DPA Log / related records	Key Staff Job Descriptions
ICO Communications	Sample Contracts
Breaches / Investigation Records	Notifications / Registrations
Fair Processing Notices / Consents	Reports e.g. Management Team

MID KENT AUDIT

Appendix II: Assurance & Priority level definitions

Assurance Ratings

Full Definition	Short Description
Strong – Controls within the service are well designed and operating as intended, exposing the service to no uncontrolled risk. There will also often be elements of good practice or value for money efficiencies which may be instructive to other authorities. Reports with this rating will have few, if any, recommendations and those will generally be priority 4.	Service/system is performing well
Sound – Controls within the service are generally well designed and operated but there are some opportunities for improvement, particularly with regard to efficiency or to address less significant uncontrolled operational risks. Reports with this rating will have some priority 3 and 4 recommendations, and occasionally priority 2 recommendations where they do not speak to core elements of the service.	Service/system is operating effectively
Weak – Controls within the service have deficiencies in their design and/or operation that leave it exposed to uncontrolled operational risk and/or failure to achieve key service aims. Reports with this rating will have mainly priority 2 and 3 recommendations which will often describe weaknesses with core elements of the service.	Service/system requires support to consistently operate effectively
Poor – Controls within the service are deficient to the extent that the service is exposed to actual failure or significant risk and these failures and risks are likely to affect the Council as a whole. Reports with this rating will have priority 1 and/or a range of priority 2 recommendations which, taken together, will or are preventing from achieving its core objectives.	Service/system is not operating effectively

MID KENT AUDIT

Recommendation Ratings

Priority 1 (Critical) – To address a finding which affects (negatively) the risk rating assigned to a Council strategic risk or seriously impairs its ability to achieve a key priority. Priority 1 recommendations are likely to require immediate remedial action. Priority 1 recommendations also describe actions the authority **must** take without delay.

Priority 2 (High) – To address a finding which impacts a strategic risk or key priority, which makes achievement of the Council's aims more challenging but not necessarily cause severe impediment. This would also normally be the priority assigned to recommendations that address a finding that the Council is in (actual or potential) breach of a legal responsibility, unless the consequences of non-compliance are severe. Priority 2 recommendations are likely to require remedial action at the next available opportunity, or as soon as is practical. Priority 2 recommendations also describe actions the authority **must** take.

Priority 3 (Medium) – To address a finding where the Council is in (actual or potential) breach of its own policy or a less prominent legal responsibility but does not impact directly on a strategic risk or key priority. There will often be mitigating controls that, at least to some extent, limit impact. Priority 3 recommendations are likely to require remedial action within six months to a year. Priority 3 recommendations describe actions the authority **should** take.

Priority 4 (Low) – To address a finding where the Council is in (actual or potential) breach of its own policy but no legal responsibility and where there is trivial, if any, impact on strategic risks or key priorities. There will usually be mitigating controls to limit impact. Priority 4 recommendations are likely to require remedial action within the year. Priority 4 recommendations generally describe actions the authority **could** take.

Advisory – We will include in the report notes drawn from our experience across the partner authorities where the service has opportunities to improve. These will be included for the service to consider and not be subject to formal follow up process.