ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	20 September 2018
REPORT TITLE	Internal Audit Report AC1904 – GDPR
REPORT NUMBER	IA/AC1904
DIRECTOR	N/A
REPORT AUTHOR	David Hughes
TERMS OF REFERENCE	2.2

1. PURPOSE OF REPORT

1.1 The purpose of this report is to present the planned Internal Audit report on GDPR.

2. RECOMMENDATION

2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

3. BACKGROUND / MAIN ISSUES

3.1 Internal Audit has completed the attached report which relates to an audit of GDPR.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report.

6. MANAGEMENT OF RISK

6.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are as detailed in the attached appendix.

7. OUTCOMES

7.1 There are no direct impacts, as a result of this report, in relation to the Local Outcome Improvement Plan Themes of Prosperous Economy, People or Place, or Enabling Technology, or on the Design Principles of the Target Operating Model.

7.2 However, Internal Audit plays a key role in providing assurance over, and helping to improve, the Council's framework of governance, risk management and control. These arrangements, put in place by the Council, help ensure that the Council achieves its strategic objectives in a well-managed and controlled environment.

8. IMPACT ASSESSMENTS

Assessment	Outcome
Equality & Human Rights Impact Assessment	An assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. As a result, there will be no differential impact, as a result of the proposals in this report, on people with protected characteristics.
Privacy Impact Assessment	Not required
Duty of Due Regard / Fairer Scotland Duty	Not applicable

9. APPENDICES

9.1 Internal Audit report AC1904 – GDPR.

10. REPORT AUTHOR DETAILS

David Hughes, Chief Internal Auditor
David.Hughes@aberdeenshire.gov.uk
(01467) 537861

Internal Audit Report

Governance

General Data Protection Regulation

Issued to:
Fraser Bell, Chief Officer – Governance
Jonathan Belford, Chief Officer – Finance
Jacqui McKenzie, Chief Officer – Customer Experience
Stephen Booth, Chief Officer – Corporate Landlord
Caroline Anderson, Information Manager
Wayne Connell, Revenue and Benefits Manager
Eleanor Sheppard, Chief Education Officer
External Audit

Date of Issue: September 2018 **Report No. AC1904**

EXECUTIVE SUMMARY

The General Data Protection Regulation (GDPR) and the majority of the provisions of the Data Protection Act 2018 (DPA 2018) came into force on 25 May 2018: together this legislation (Data Protection legislation) replaced the Data Protection Act 1998 (DPA 1998).

The legislation introduces several major changes to former data protection legislation, including, but not limited to, increased accountability and transparency requirements, strengthened rights for individuals in relation to their own personal data, and greater penalties for breaching the requirements of the Data Protection legislation, up to a maximum of €20 million or 4% of turnover.

The objective of this audit was to provide assurance that the Council has adequate arrangements in place, that are understood throughout the organisation, to protect the Council's information.

In general, the audit found that adequate policy and procedures were in place, describing the Council's approach to managing information held be it. In order to enhance these, Governance has agreed to establish detailed procedures relating to individual's rights to data portability, and automated decision making and profiling.

A comprehensive range of training is available, and while only 44% of staff had completed the mandatory Information Governance training as at 11 September 2018, exception reporting is in place to advise Chief Officers of those employees yet to complete the training so that they can take appropriate corrective action.

The Council has adequate arrangements in place in terms of: a Data Protection Officer; registration with the ICO; data protection impact assessments; the records of processing activities; data breach monitoring; data retention guidance; freedom of information requests; postage guidance; and confidential waste.

Revised privacy notices were found to comply with the requirements of GDPR, however some paper forms in use at the time of the audit were found to refer to previous data protection legislation and some school parental permission forms lacked privacy notices. The historic forms have largely been replaced with updated versions and the respective Services have agreed to update the Penalty Charge Notice and pupil photo permission form to include a GDPR compliant privacy notice.

Contracts with the Council's data processors are currently being updated using a risk based approach (those contracts which are higher risk, e.g. social care, are being updated first). Higher risk contracts have been updated and Commercial and Procurement Services has agreed to ensure all data processor contracts are updated to reflect the requirement of GDPR.

Other recommendations have been agreed in relation to updating the Surplus Property procedures to require documents containing personal data to be removed from vacated premises and to ensuring a review of Information Sharing Agreements is completed to determine any necessary GDPR updates required to these agreements.

1. INTRODUCTION

1.1 The General Data Protection Regulation (GDPR) and the majority of the provisions of the Data Protection Act 2018 (DPA 2018) came into force on 25 May 2018: together this legislation (Data Protection legislation) replaced the Data Protection Act 1998 (DPA 1998).

1.2 The GDPR regulates the processing of personal data from which a living individual could be identified. Processing of data includes: collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, combining with other data, restriction, erasure or destruction. The GDPR applies to any computerised or manual records containing personal information about living and identifiable people, and requires that appropriate technical and organisational measures are taken to ensure compliance with the Regulation. No personal data may be processed unless the Data Controller (organisation alone or jointly with others, determining the purposes and means of processing of personal data e.g. the Council) has identified an appropriate legal basis or bases, which meets the requirements of the GDPR. The GDPR provides derogations to EU member states on some elements of how Data Protection law will work domestically. The UK has enacted the Data Protection Act 2018 for this purpose. The DPA 2018 also sets the law around types of personal data processing not covered in the GDPR (for example, the processing of personal data for law enforcement purposes).

1.3 The legislation introduces several major changes to former data protection legislation, including, but not limited to, increased accountability and transparency requirements, strengthened rights for individuals in relation to their own personal data, and greater penalties for breaching the requirements of the Data Protection legislation, up to a maximum of €20 million or 4% of turnover.

1.4 The objective of this audit was to provide assurance that the Council has adequate arrangements in place, that are understood throughout the organisation, to protect the Council's information.

1.5 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Caroline Anderson (Information Manager), and Helen Cannings, Catriona Sim and Susan Patterson (Information Management Team).

2. FINDINGS AND RECOMMENDATIONS

2.1 Written Procedures and Training

2.1.1 Comprehensive written procedures and guidance which are easily accessible by all members of staff can reduce the risk of errors and inconsistency. They are beneficial for the training of current and new employees and provide management with assurance that correct and consistent instructions are available to staff, important in the event of an experienced employee being absent or leaving. They have increased importance where new systems or procedures are being introduced.

2.1.2 On the Council's intranet ('the Zone') the Service provides policy, procedures and guidance for the management of information – primarily through the 'Managing Information Handbook'. The Service has updated the policy, procedures and guidance to reflect the requirements of GDPR.

2.1.3 The Service has made available both face-to-face and e-learning data protection training through the Council's Online Interactive Learning (OIL) platform. Face-to-face training sessions included the following (attendance numbers in brackets):

- Service specific changes to data protection law (825)
- Elected Members training on changes to data protection law (36)
- General session on the changes for data protection law (137)
- Data protection impact assessments briefing and training sessions (32)
- Information asset owner training (181)
- Managing information session (1)
- Updating privacy notices (70)

2.1.4 The OIL course entitled 'Information Governance Training' became available in July 2018 and as at 11 September 2018 was completed by 3,927 (44%) members of staff. These completion rates have been broken down by function below:

Function	Current Staff	Number of Staff completed OIL course	Percentage
Social Care	584	277	47%
Commissioning	102	80	78%
Customer	1,103	913	83%
Governance	72	69	96%
Operations	6,414	2,187	34%
City Growth	241	88	37%
Strategic planning	166	116	70%
Resources	276	197	71%
Total	**8,958**	**3,927**	**44%**

2.1.5 Information Governance mandatory training completion rates are being sent to Chief Officers on a weekly basis. In addition, monthly exception reports are being sent to Chief Officers, with details of employees yet to complete the Information Governance training, for the purposes of ensuring training is completed as required. Elected Members are not required to complete the OIL course however further face-to face data protection training is scheduled to be delivered on the 20 September and 1 October 2018 for Elected Members yet to receive training.

2.2 **Data Protection Officer and ICO registration**

2.2.1 Under GDPR the Council is required to appoint a Data Protection Officer responsible for monitoring internal compliance amongst other tasks. The Council has appointed an interim Data Protection Officer and intends to recruit an individual to this role in the coming months. Further, the Council must, as an organisation processing personal data, pay a data protection fee to the Information Commissioners Office (ICO) (the UK's independent body to uphold information rights). This was verified through an examination of the ICO's register of fee payers. In addition, it was verified that all Tier 1 and 2 ALEOs, which are required to pay a data protection fee to the ICO, have done so. These ALEOs are separate data controllers from the Council and are responsible for their own data protection compliance arrangements.

2.3 **Privacy Notices**

2.3.1 In accordance with GDPR Article 13, where personal data relating to a data subject is collected, the Council uses privacy notices to: explain the purposes of processing; the legal basis for processing; the data subjects rights in relation to their personal data held by the Council; whether the data will be shared with any other parties; whether there is any automated decision making or profiling using the personal data; the retention period; and the contact details of the Data Protection Officer, responsible for monitoring the Council's compliance with Data Protection legislation.

2.3.2 The Council's 'Managing Information Handbook', available from the Zone, identifies the procedure for identifying where privacy notices are required and how these should be prepared. Internal Audit selected a sample of 15 privacy notices and in each case these had been updated in accordance with GDPR and the handbook.

2.3.3 To ensure the paper forms completed by customers have been updated to include privacy notices compliant with GDPR, a selection of 19 forms available from the Marischal College Customer Service Centre in August 2018 were inspected by Internal Audit. The following was noted:

- 7 forms had privacy notices which complied with GDPR
- 1 of the forms made reference to the 'Data Protection Act' but did not meet the requirements of GDPR
- 11 forms contained reference to the DPA 1998

Recommendation
The Service should ensure all forms have been updated to include privacy notices compliant with GDPR.

Service Response / Action
Whilst forms were being updated the Customer Service Centre was issuing copies of the old forms. This has now been resolved and all forms have been replaced with the updated copies.

The Penalty Charge Notice forms will be further revised following the update to the privacy notice which is currently underway.

Implementation Date	Responsible Officer	Grading
October 2018	Revenue and Benefits Manager	Significant within audited area

2.3.4 The introduction of GDPR necessitated that employees also be made aware of how their personal data is used via a privacy notice. A communication was emailed to all third tier managers for dissemination amongst their teams, providing guidance on accessing the

updated employee privacy notice, and a similar message was also posted to the Zone. Employees were encouraged to contact the Council's Data Protection Officer with any further queries they have. The privacy notice adequately described the personal data collected; types of processing; legal basis for processing; and rights of the individual in relation to their personal data held by the Council.

2.4 **Individual's Rights**

2.4.1 Under GDPR an individual has 8 defined rights:

- The right to be informed (privacy notices)
- The right of access (subject access)
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

2.4.2 The Council's 'Managing Information Handbook' confirms that the Council has implemented policies and procedures for each of the above rights, except the right to data portability and the rights in relation to automated decision making and profiling. Whilst reference is made to each, there is no detailed procedure in place to ensure compliance with these rights. The Managing Information Handbook refers to a section of the handbook where relevant procedures can be found, however this was absent from the handbook. This increases the risk the Council may not adequately address these rights.

Recommendation
The Service should ensure procedures are in place to address all rights of individuals as described by GDPR.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
December 2018	Information Management Team Leader	Important within audited area

2.4.3 Internal Audit obtained a listing of all requests for erasure, access, rectification and data portability. Under GDPR the Council must provide responses to such reasonable requests within 1 month of receipt and may only charge a fee if the request is deemed manifestly unfounded or excessive. A sample of 10 subject access requests was tested and it was confirmed these were responded to within the required timeframe and that if a fee was charged, this was appropriate.

2.5 **Data Processors**

2.5.1 GDPR Article 28(3) and section 59(5) of the DPA 2018 require that where a data controller such as the Council uses a third party to process personal data (processor), the processing should be governed by a contract, binding the processor to the controller and setting out the subject matter and duration of processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.

2.5.2 The updating of contracts is currently being performed using a risk based approach (those contracts which are higher risk, e.g. social care, are being updated first). Of a sample of 12 updated contracts, each was found to have been appropriately updated in accordance

with GDPR Article 28 and had been approved by both parties. A recommendation has been made here for tracking purposes.

Recommendation
The Service should ensure all relevant contracts with data processors are updated to reflect the requirements of GDPR Article 28.

Service Response / Action
Contracts were prioritised based on the extent that personal information is shared with contractors. All social care contracts have been reviewed (209). 159 have had either a variation or a new contract issued with GDPR compliant clauses – 101 of these have been fully signed by both the Council and Provider, with the remaining 58 being in the issue / signing process. 50 remain to be reviewed and varied or a new contract issued – these include 25 National Care Home Contracts where the Council has recently received the preferred wording from Scotland Excel/COSLA. As regards all other contracts, the Council is continuing to prioritise these based on whether or not personal information is shared with the contractor. The Council's Contract Register is being used as the basis for this and work is progressing to update all contracts.

Implementation Date	Responsible Officer	Grading
December 2018	Team Leader – Commissioning	Important within audited area

2.6 **Data Protection Impact Assessments**

2.6.1 The Council has a legal requirement to carry out a data protection impact assessment (DPIA) for any type of processing that is likely to result in a high risk to the rights and freedoms of individuals. Within the Council's 'Managing Information Handbook', guidance is provided to ensure that officers are aware of when DPIA's are required and how these should be performed. This also includes a template for the completion of DPIA's. Further, the Council maintains an up-to-date register of all DPIA's in progress and completed, with these being sequentially numbered, to facilitate tracking of progress.

2.6.2 Since the introduction of GDPR, the Council has completed 6 DPIA's, with a further 28 currently in progress. Three completed DPIA's were obtained and it was confirmed that these had been fully completed, and that each was signed and approved as appropriate by the Data Protection Officer.

2.7 **Data Breaches**

2.7.1 The Information Governance Group (IGG), responsible for supporting and driving the broader information governance agenda, reviews the Council's data protection compliance, on a quarterly basis. A report is reviewed quarterly by the IGG, which includes response times to data subject access and the number of data protection breaches and complaints. This is also reported annually to the Audit, Risk and Scrutiny Committee (most recently reported on 26 September 2017 for the period July 2016 – June 2017). The next annual report, covering the period July 2017 to June 2018, will be reported to Audit, Risk and Scrutiny Committee on 25 September 2018. Internal Audit reviewed copies of the last 4 available quarterly reports and the following was noted:

	Breaches	*Self-Reports to ICO*	*Data Handling Complaints*
Apr – Jun 17	10	0	0
Jul – Sep 17	12	0	1
Oct – Dec 17	7	0	2
Jan – Mar 18	22	0	0
Total	***51***	***0***	***3***

2.7.2 The types of breaches within this period were either the result of human error or unauthorised disclosure (e.g. incorrect email recipient). In this period there were no instances resulting in data loss or security failures.

2.7.3 More recently, an incident occurred in July 2018 in which the P11D forms for 837 current and 110 former employees were distributed to incorrect recipients. As such, the Information Security Incident Reporting procedure was followed and the breach reported to the ICO. Employees were also made aware of the breach by letter and an announcement on the Zone. Internal Audit inspected all records relating to the breach and the report prepared by the Service. It was agreed that the correct procedure was undertaken and that the breach was reported to the ICO as required within the correct timeframe (72 hours). Potential actions the ICO may take include investigating the breach and issuing a fine.

2.8 Information Asset Register

2.8.1 Article 30 of GDPR requires that each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following: the name and contact details of the controller; the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed (including internationally); details of transfers to a third country; time limits for erasure (where possible); and a general description of the technical and organisational security measures (where possible).

2.8.2 The Council maintains an Information Asset Register which was found to be up to date. The processing activities recorded in relation to personal data held was found to comply with the requirements of GDPR. On inspection of the Information Asset Register it was confirmed that through the ICT Service Now platform, certain employee information is stored internationally in the Netherlands, an EU member state where GDPR applies.

2.9 Data Retention

2.9.1 Article 5(1)(e) of GDPR requires that data should not be held for longer than it is actually needed. The Council must therefore have reasoning for the retention period for each item of data held.

2.9.2 The Council maintains a comprehensive data retention schedule which is easily accessible by all employees. On inspection of the schedule it was confirmed that appropriate guidance is being given to ensure data is held for appropriate time periods, with reasons included for retention duration (either legislative or business requirement e.g. business requirement to retain for historical reasons). Instruction for the method of disposal of the information is also given. The Records Retention and Disposal Schedule was found to adequately describe the reasons for retention of personal data.

2.10 Education and Social Work

2.10.1 Given the sensitive high risk nature of certain types of personal data (e.g. social work / education records) it is important that these are stored securely and that only authorised

personnel can access these. Internal Audit visited 2 primary schools, 1 secondary school and 3 social work offices. At each of these visits, inspections were undertaken to ascertain how personal data was being collected and stored, and to ensure that personal data was stored securely and only accessible by authorised individuals. No exceptions were noted in relation to data security.

2.10.2 A letter was sent to parents and carers by the then Interim Head of Education and Inclusion explaining the impact of GDPR. This described the pupil personal data that is collected, the legal basis for this and the rights of parents in relation to personal data held by the Council.

2.10.3 The pupil enrolment form collects personal data, including special category personal data, on pupils. A GDPR compliant privacy notice is present on the enrolment form which describes the legal basis for collecting this data. The enrolment form also states pupil data may be shared with partners of the Council where data sharing agreements are in place. It was however noted during the visits to schools that parental permission forms (for matters such as photography, videos and sharing information e.g. for the NHS Dental Inspection Programme) are prepared by each school without privacy notices. Failure to provide appropriate explanation as to why personal data is being collected and the legal basis for processing that data may result in fines or reputational damage.

Recommendation
The Service should consider issuing standard permission forms for all schools to use, that include privacy notices compliant with GDPR where required.

Service Response / Action
Agreed.

Quality Improvement Officers will look at GDPR at the first 2018/19 Quality Assurance visit so that we can be confident in the use of revised enrolment forms which includes a GDPR compliant privacy notice and notifies parents of data sharing arrangements.

New photo permission privacy notices are currently being consulted on to ensure the range of reasons for pupil photographs are covered in the final photography consent privacy notice.

The Service is currently in discussion with the NHS in relation to the dental / ChildSmile privacy notice. No dental or ChildSmile forms will be issued through school until we have a privacy notice from the NHS.

Implementation Date	Responsible Officer	Grading
November 2018	Chief Education Officer	Important within audited area

2.11 **Confidential Waste**

2.11.1 The current confidential waste contract was awarded for a period of 6 months running from 26 April 2018 to 25 October 2018. The contract is for the provision of confidential waste bins, and collection and disposal of waste within these bins on a weekly basis. The Building Manager for Marischal College confirmed that regular inspections are undertaken to ensure these bins are not overflowing or that disposed waste is accessible. Further, when additional confidential waste bags are used during larger clear-outs these are sealed and stored in a locked cage in the mail room within Marischal College. These storage arrangements were found to be adequate. In addition, a sample of confidential waste bins was inspected, and these were not overfilled with confidential waste being inaccessible.

2.12 **Property disposals**

2.12.1 To avoid data protection breaches, the Council must ensure that documents containing personal data are removed from Council premises prior to property being disposed of. A Surplus Property Handover form must be completed and submitted to Corporate Landlord by the relevant Service when a property is being vacated. The form contains boxes which must be ticked to indicate whether or not the property is empty. However, the form does not require confirmation that all documentation containing personal data has been removed from the property, meaning such documents may be inadvertently left behind.

Recommendation
The Service should update Surplus Property procedures to require documentation containing personal data be removed from premises being vacated.

Service Response / Action
Agreed. The Service will update the property hand over form to specifically include reference to the removal of documentation including personal data.

Implementation Date	Responsible Officer	Grading
December 2018	Property Estates Manager	Important within audited area

2.13 **Freedom of Information**

2.13.1 Under the Freedom of Information (Scotland) (FOI) Act 2002 the public is entitled to make requests for information held by the Council. However, when providing this information the Council must ensure that data protection legislation is complied with. Internal Audit examined the procedures in place for responding to FOI requests to ensure this complied with data protection requirements. Further, a sample of 40 FOI request responses available on the Council's website were examined to ensure these complied with data protection legislation. No exceptions were noted from this testing and the procedures were appropriate.

2.14 **Mail**

2.14.1 The Council uses three mail providers; one for all first class, recorded, signed for and air mail; another for second class mail; and another for legal mail. The Managing Information handbook includes a procedure describing checks to be undertaken before sending information by post and requires 'sensitive or special category personal information' to be sent using a tracked postal service, reducing the risk personal data will be sent to the wrong recipient.

2.15 **ICT Equipment**

2.15.1 The loss of ICT equipment can result in data protection breaches. The Council's Managing Information Handbook identifies the procedures which should be undertaken were an individual to lose ICT equipment. This includes contacting ICT who can then deactivate the device. Further, the inappropriate usage of removable storage devices (e.g. memory stick) is also addressed. The policy requires that only Council issued removable storage devices should be used as these are encrypted, reducing the chance of data loss. Data breach and cyber attack prevention was reviewed as part of the Major IT Business Systems audit AC1810 and has therefore not been examined further as part of this audit.

2.16 **Data Sharing**

2.16.1 The Council holds several data sharing agreements with different organisations, including Police Scotland, the NHS and the Scottish Government. Some of these agreements involve multiple parties, sometimes even involving all 32 Scottish local authorities. The conclusion or updating of such agreements will therefore often depend upon input from a number of different parties. Each of these agreements is tracked on an Information Sharing Agreement Register which identifies all parties involved. During the review of privacy notices it was confirmed that these sharing agreements are being appropriately disclosed where required. Further, the Service is undertaking a review of these Information Sharing Agreements to assess whether or not they comply with GDPR. A recommendation is made here for tracking purposes.

Recommendation
The Service should ensure all data sharing agreements are reviewed to assess whether or not they comply with GDPR and produce a plan for any necessary updating of such agreements.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
December 2018	Team Leader – Governance	Important within audited area

AUDITORS: D Hughes
A Johnston
J Grigor

Appendix 1 – Grading of Recommendations

GRADE	DEFINITION
Major at a Corporate Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss, or loss of reputation, to the Council.
Major at a Service Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss to the Service/area audited. Financial Regulations have been consistently breached.
Significant within audited area	Addressing this issue will enhance internal controls. An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on a system's adequacy and effectiveness. Financial Regulations have been breached.
Important within audited area	Although the element of internal control is satisfactory, a control weakness was identified, the existence of the weakness, taken independently or with other findings does not impair the overall system of internal control.