Aberdeenshire COUNCIL Business Services

REPORT TO AUDIT COMMITTEE – 17 SEPTEMBER 2020

DATA PROTECTION OFFICER ANNUAL REPORT

1 Reason for Report / Summary

1.1 The Committee requested that an Information Governance report be provided on an annual basis.

2 Recommendations

Audit Committee is recommended to:

2.1 Discuss and acknowledge the Data Protection Officer Annual Report for 2019/20.

3 Purpose and Decision Making Route

3.1 Purpose

3.1.1 At a forward planning workshop, the Committee requested that an Information Governance report be provided to Committee on an annual basis. Information Governance has since been split with the Data Protection function having transferred to Legal & Governance and Information/Cyber Security remaining in ICT. The Data Protection Officer has therefore prepared a Data Protection Annual Report for Committee. A further report will be provided to Committee in due course by ICT covering Information/Cyber Security.

3.2 Decision Making Route

3.2.1 This Annual Report has not previously been considered by this or another Committee.

4 Discussion

4.1 The General Data Protection Regulation (GDPR) and Data Protection Act (2018) both came into force on 25th May 2018, increasing organisational data protection obligations, and accountability, as well as enhancing individual's data protection rights. Processes and working practices across the Council have since been adapted to ensure compliance. The DPO annual report from May 2019 to May 2020 is attached at Appendix 1 to this report.

4.2 The DPO produces a monthly management report for Directors outlining identified issues and concerns which are usually addressed by services. Overall, while the DPO feels the Council does not have any significant risks in this service area, there is some room for improvement, as detailed at 4.3 to 4.8.

4.3 The General Data Protection Regulation (GDPR) requires all public authority data controllers to designate a Data Protection Officer (DPO). The DPO must be designated based on professional qualities and expert knowledge of data protection law and practices, and the ability to fulfil the statutory tasks set out in the GDPR. Since the GDPR came into force in May 2018, Andrew Lawson has been designated 'Acting DPO' on behalf of Aberdeenshire Council (including all 170 schools), Aberdeenshire Licensing Board, Aberdeenshire Integrated Joint Board, and the Aberdeenshire Returning Officer. Despite an internal audit recommendation, due for completion by July 2019, recommending the Council appoint a full time DPO and consider moving the DPO to Legal, this recommendation has yet to be addressed in full. A revised completion date of Spring 2020 has also been missed but the Legal & Governance service are in the process of progressing this matter.

The Council should set a firm date by when a DPO will be appointed on a substantive basis.

4.4 The target percentage for completion of Data Protection Awareness Training is 90%. As of June 2020, 69.6% of staff and 42% of Councillors have completed mandatory training.

All Council Services, and, where necessary, Councillors, should take action to comply with the previously received formal undertaking from the ICO, and internal audit recommendation, to ensure completion percentage is above 90%.

4.5 In the previous Data Protection Officer's Annual Report, the DPO expressed concern that 19% of requests being issued late was too high and that there was room for improvement. While there has been some improvement during the past year with the percentage lately having decreased to 16%, the DPO feels there is still further room for improvement.

Council Services should take action to increase the number of responses to requests issued on time to above 90% by ensuring Services have appropriate resource in place to meet statutory timeframes.

4.6 In the 2018/19 Data Protection Officer's Annual Report, the DPO expressed concern regarding the number of email-related data breaches, advising of a recommendation made to ICT to review technical measures currently in place with a view to introducing additional technical measures, where appropriate, to help drive-down the number of breaches. Despite ICT agreeing to undertake a review, and the DPO providing a copy of a report from a similar review undertaken by Aberdeen City Council to assist with the process, this has not yet taken place.

As per recommendation made in DPO Annual Report 2018/19, Customer and Digital Services should take action to review technical measures currently in place with a view to introducing additional technical measures, where appropriate, to help drive down the number of email-related data breaches.

4.7 An increasing number of DPIAs are not being seen through to completion. Some DPIAs have now been in draft for more than one year and the DPO has particular concerns where data processing commences in advance of a DPIA having been finalised and approved.

All Council Services should ensure DPIAs are undertaken, when necessary, and ensure DPIAs are seen through to completion.

4.8 The DPO expressed concern at the Council's decision to ask individuals submitting Data Protection and Freedom of Information requests to consider withdrawing their request until after the COVID-19 pandemic. The DPO reminded the Council of its obligations insofar as both Data Protection and Freedom of Information legislation are concerned.

The Council should consider discontinuing the practice of discouraging individuals from submitting information requests.

5 Council Priorities, Implications and Risk

5.1 The report helps deliver Council Priority – Our People: right people, right places, right time.

5.3 The table below shows whether risks and implications apply if the recommendation(s) is(are) agreed.

Subject	Yes	No	N/A
Financial			X
Staffing			X
Equalities			X
Fairer Scotland Duty			X
Town Centre First			X
Sustainability			X
Children and Young People's Rights and Wellbeing			X

5.4 An equality impact assessment is not required because this report informs the Committee of the planned reporting activity and does not have a differential impact on any of the protected characteristics.

5.5 The following risks have been identified as relevant to this matter on a Corporate Level: Corporate Risk Register.

ACORP002: Changes in legislation and regulation
ACORP006: Reputation Management
ACORP008: Data Protection and Cyber Security

6 Scheme of Governance

6.1 The Head of Finance and Monitoring Officer within Business Services have been consulted in the preparation of this report and are satisfied that the report complies with the Scheme of Governance and relevant legislation.

6.2 The Committee is able to consider on this item in terms of Section G.1.1 of the List of Committee Powers in Part 2A of the Scheme of Governance as the report relates to matters delegated to the Committee.

Ritchie Johnson
Director of Business Services

Report by A Lawson, Data Protection Officer
Date: 26 August 2020

Appendix 1

Aberdeenshire COUNCIL

DATA PROTECTION OFFICER'S ANNUAL REPORT

MAY 2019 TO MAY 2020

Table of Contents

Foreword

In the second year of the General Data Protection Regulation (GDPR), many of the changes brought about by the GDPR, and Data Protection Act (2018), enhancing individual's rights, have now been fully embedded into working practices across the Council.

The main unanticipated challenge during the past year has been Covid-19 with a resulting temporary but significant increase in the number of requests for advice. The DPO has had to ensure that Data Protection has not been cited incorrectly as a barrier to proportionate and necessary data sharing, while of course balancing that with the continuing need to protect and secure personal data and ensure data processing remains transparent.

The past year has seen a marked drop in the number of staff with up-to-date Data Protection training, a small increase in the number of data breaches arising, and perhaps less urgency in undertaking and completing DPIAs. It is important for the Council to continue to pay sufficient regard to Data Protection not only to ensure individual's rights are upheld but also due to the fact enhanced enforcement powers granted to the ICO, including the power to levy a fine of €20,000,000 or up to 4% of annual global turnover, whichever is larger, have not gone away.

During the past year, the Council's Data Protection, Freedom of Information and Information and Records Management Governance functions transferred from ICT to Legal and Governance, with Information Security remaining within ICT. These changes have resolved several conflicts of interest and are welcomed by the DPO.

Andrew Lawson
Data Protection Officer

The Role of the DPO

The General Data Protection Regulation (GDPR) requires all public authority data controllers to designate a Data Protection Officer (DPO). The DPO must be designated based on professional qualities and expert knowledge of data protection law and practices, and the ability to fulfil the statutory tasks set out in the GDPR.

The designated Data Protection Officer must directly report to the highest management level, must not receive instructions regarding the exercising of statutory tasks, and shall not be penalised or dismissed for performing those tasks. The controller must support the DPO in performing his tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations.

Since the GDPR came into force in May 2018, Andrew Lawson has been designated 'Acting DPO' on behalf of Aberdeenshire Council (including all 170 schools), Aberdeenshire Licensing Board, Aberdeenshire Integrated Joint Board, and the Aberdeenshire Returning Officer.

Despite an internal audit recommendation, due for completion by July 2019, recommending the Council appoint a full time DPO and consider moving the DPO to Legal, this recommendation has yet to be addressed in full. A revised completion date of Spring 2020 has also been missed.

The Council should set a firm date by when a DPO will be appointed on a substantive basis.

Data Protection Policy

The Council's Data Protection Policy was re-written for the GDPR and approved by Business Services Committee on 14th June 2018. The policy was last reviewed on 7th January 2020 when an amendment was made increasing the frequency of Data Protection training from every three years to every two years in-line with an Information Commissioner's Office (ICO) recommendation and current best practice.

Data Protection Awareness

In April 2018, Data Protection awareness training was refreshed for the GDPR, and made available to staff via ALDO. Awareness training consists of six short videos and a multiple-choice assessment, with an overall duration of 30 minutes. During the second year of the GDPR, three of the six training modules have been updated to reflect current requirements.

The target percentage for completion of Data Protection Awareness Training is 90%. As of June 2020, 69.6% of staff and 42% of Councillors have completed mandatory training.

All Council Services, and where necessary Councillors, should take action to comply with the previously received formal undertaking from the ICO, and internal audit recommendation, to ensure completion percentage is above 90%.

Data Protection Awareness Training Completion by Service:

Service	Total number of staff required to undertake training	Total number of staff who have completed training	Total number of staff outstanding	Percentage complete
Business Services	899	621	278	69.1
Education & Children's Services	11685	8029	3656	68.7
Health & Social Care Partnership	2502	1814	688	72.5
Infrastructure Services	1396	998	398	71.5
Chief Executive	7	7	0	100.0
Councillors	69	29	40	42.0
Total	**16558**	**11498**	**5060**	**69.4**

Stats as of June 2020

Information Rights (including Access Requests)

Under the GDPR, individuals have a number of rights including the right to be informed, the right to make an access request, the right to rectification, the right to erasure (the right to be forgotten), the right to restriction of processing and the right of data portability. Individuals' rights are covered within Council Data Protection Policy.

Number of valid requests received during 2019-2020:

Right	Number received	Number of responses issued on time
Access Requests	120	101
Rectification Requests	3	3
Erasure Requests	1	1
Restriction of Processing Requests	0	0
Data Portability Requests	0	0

In the previous Data Protection Officer's Annual Report, the DPO expressed concern that 19% of requests being issued late was too high and that there was room for improvement. While there has been some improvement during the past year with the percentage late having decreased to 16%, the DPO feels there is still further room for improvement. In comparison, for the same period, only 4% of Freedom of Information (FOI) responses were issued late. FOI performance is currently better than Subject Access Request (SAR) performance even though fines cannot be imposed for late FOI responses but can for late SAR responses.

Council Services should take action to increase the number of responses to requests issued on time to above 90% by ensuring Services have appropriate resource in place to meet statutory timeframes.

While the Council has seen a small decrease in the total number of requests received during the past year, the DPO feels this decrease is likely due to data subjects having been discouraged from making requests, by the Council and by the ICO, for a period of two months during the Covid-19 lockdown. Had such discouragement not taken place it is likely the Council would have seen a further increase in the overall number of requests received.

Number of valid Access Requests received by year:

Year	Number of access requests received
2019-2020	120

2018-2019	130
2017-2018	77
2016-2017	43

As well as processing requests received from members of the public and staff, the Council also processes requests made under Schedule 2 of the Data Protection Act (2018), primarily from Police Scotland, seeking information held to assist with the prevention and detection of crime and the apprehension and prosecution of offenders. The number of valid Schedule 2 requests received has decreased in the past year.

Number of valid Schedule 2 requests received by year:

Year	Number of S2 requests received
2019-2020	145
2018-2019	172
2017-2018	57
2016-2017	31

Data Breaches

During the second year of the GDPR, the number of suspected data breaches reported to the DPO, which have subsequently been confirmed by the DPO, has increased from 67 to 70; a 4% increase from previous year.

Number of confirmed data breaches reported by year:

Year	Number of confirmed data breaches
May 2019 – May 2020	70
May 2018 – May 2019	67
May 2017 – May 2018	28
May 2016 – May 2017	8
May 2015 – May 2016	8

A significant proportion of data breaches arise due to human error and lack of due care. Lack of due care when using email, accounts for 52% of confirmed data breaches in the past year; a 10% increase from previous year.

In the 2018/19 Data Protection Officer's Annual Report, the DPO expressed concern regarding the number of email-related data breaches, advising of a recommendation made to ICT to review technical measures currently in place with a view to introducing additional technical measures, where appropriate, to help drive-down the number of breaches. Despite ICT agreeing to undertake a review, and the DPO providing a copy of a report from a similar review undertaken by Aberdeen City Council to assist with the process, this has not yet taken place.

As per recommendation made in DPO Annual Report 2018/19, Customer and Digital Services should take action to review technical measures currently in place with a view to introducing additional technical measures, where appropriate, to help drive down the number of email-related data breaches.

Data breaches by data breach type:

Data Breach by Type	Number of confirmed data breaches 2019/20	Number of confirmed data breaches 2018/19
Email - incorrect external recipient	18	14
Postal mail - incorrect address	8	12
Email - failure to use BCC	12	9
Email - incorrect attachment	6	5
Inappropriate disclosure to third party (written & verbal)	12	5
Failure to redact appropriately (FOI responses)	1	2
Failure to redact appropriately (other)	1	2
Postal mail - Incorrect personal data contained in letter	5	4
Disclosure to third party without having contract in place	1	2
Failure to dispose of personal data into Confidential Waste	0	2
Postal mail - Mail lost in delivery (Royal Mail)	0	2
Access Rights set incorrectly allowing inappropriate access to data	0	1
Document missing after being left in an insecure area	0	1
Excessive data provided to third party for test purposes	0	1
File saved to a pupil-accessible drive in error	0	1
Lost unencrypted USB drive	1	1
Personal data uploaded into system against incorrect individual	0	1
Data Processor breach	2	1
Loss of paper file	1	0
Upload to Social Media without consent	2	1
Total	70	67

While the number of data breaches arising within Education & Children's Services is more than triple that arising within each of the other Services, on taking the number of staff within each Service into consideration, this highlights a greater issue within both Business Services and Infrastructure Services. Please note that there would appear to be a statistically significant increase in the number of confirmed data breaches arising within Infrastructure Services.

Data breaches arising by Service:

Data Breaches by Service	Number of confirmed data breaches 2019/20	Number of confirmed data breaches 2018/19
Education & Children's Services	41	40
Business Services	10	10
Health & Social Care Partnership	6	10
Infrastructure Services	13	7
Total	70	67

Data breaches arising by Service per 1000 staff:

Data Breaches by Service	Number of confirmed data breaches per 1000 staff 2019/20	Number of confirmed data breaches per 1000 staff 2018/19
Business Services	11	11
Infrastructure Services	9	5
Education & Children's Services	4	5
Health & Social Care Partnership	2	4

Most data breaches arising fall below the threshold for reporting to the ICO. During the second year of the GDPR, only three data breaches were deemed by the DPO to require reporting to the ICO. Further detail concerning these three data breaches can be found at Appendix 1.

Data Protection Complaints

In the second year of the GDPR, the Council Feedback Team took on the role of administering data protection complaints on behalf of the DPO, seeking input as necessary from relevant service(s) and the DPO.

Number of formal complaints received:

Data Breaches by Service	Number of complaints received
2019/20	9
2018/19	12

Source: Council Feedback Team

Data Protection Impact Assessments

The GDPR introduced a new requirement for Data Controllers to undertake a Data Protection Impact Assessment (DPIA) to help identify and minimise data protection risk where processing is likely to result in a high risk to individuals.

During the second year of the GDPR, numerous DPIAs were undertaken by Council Services, all of which identified privacy risks and detailed how these risks were to be subsequently reduced or mitigated. DPIAs are proving to be a useful privacy risk identification and reduction mechanism.

During 2019/20, many DPIAs were submitted including in relation to Planning Virtual Site Visits, Recycling Permits, Corporate Arrears System, AVCs, Edukey, and School Transport.

While no DPIAs have been rejected by the DPO during 2019/20, a growing number of DPIAs are not being seen through to completion. Some DPIAs have now been in draft for more than one year and the DPO has particular concerns where data processing commences in advance of a DPIA having been finalised and approved. Outstanding DPIAs include GLOW, Employee Benefits, ShowMyHomework and Caledonian System.

All Council Services should ensure DPIAs are undertaken, when necessary, and ensure DPIAs are seen through to completion.

Data Sharing

During the second year of the GDPR, a formal Data Protection Agreement review process was put in place to satisfy an internal audit recommendation.

The DPO has reviewed and provided feedback in relation to numerous draft Data Sharing Agreements including: Caledonian System, Apply4Homes, Children's Hearings Service, Drug and Alcohol Information Sharing, PIE Census, European Structural Funds, Grampian Region Child Abuse, Housing First, iVPD Flagging, MAPPA, National Entitlement Card, NESCol, Northern Alliance Data Sharing, Source Social Care Data Sharing, PREVENT, Skills Development Scotland, and many more.

Covid-19

As per other Council services, the Council's Data Protection function has been impacted by Covid-19.

During lockdown, the DPO has been actively involved in reviewing relevant Data Sharing Agreements for the sharing of personal data relating to shielded individuals and other individuals at risk. The DPO has also pro-actively assisted with the production of relevant Covid-19 privacy notices for the public, volunteers and for staff.

Guidance was also provided reminding staff that data protection obligations continue to apply in full despite Covid-19, as some staff were found to be disregarding the requirement to appropriately secure personal data and to provide privacy notices.

At the start of lockdown, the DPO set up weekly Skype drop-in sessions for Service Data Protection reps to assist reps with any Covid-19 related queries.

The DPO has also been involved in reviewing new ways of working arising because of Covid-19, via Data Protection Impact Assessments. At the time of writing this report, DPIAs have been completed and signed-off for a new Waste Recycling Booking Service and Planning Virtual Site Visits.

The DPO expressed concern at the Council's decision to ask individuals submitting Data Protection and Freedom of Information requests to consider withdrawing their request until after the pandemic. The DPO reminded the Council of its obligations insofar as both Data Protection and Freedom of Information legislation are concerned. At the time of writing this report, individuals are still being discouraged from making information requests despite individuals continuing to have the legal right to do so.

The Council should consider discontinuing the practice of discouraging individuals from submitting information requests.

Working Groups

During the second year of the GDPR, the DPO has been an active participant in several working groups.

SOLAR Data Protection/FOI Working Group – a working group consisting of Data Protection and Freedom of Information representatives from the 32 Scottish Local Authorities. This is an extremely useful working group which discusses matters of shared concern and which is also used to share effort such that all 32 Scottish Local Authorities do not have to re-invent the same wheel. During the pandemic, this group has increased the frequency of meetings which now take place via Webex.

The Data Protection Working Group – the DPO chairs this internal group which includes Data Protection and Freedom of Information Service representatives. During the past year, the DPO has formalised this group, given discontinuation of the Information Management Operational Group, with this group now meeting monthly with secretarial support received from Business Support Admin.

Future Matters

Brexit

The Council has limited personal data located out with the UK both in the EEA and in the United States. There remains uncertainty around Brexit which could impact on data flows to/from the UK. The Council has already undertaken a review of personal data located out-with the UK to identify all such data. Relevant contracts may need to be amended with revised clauses depending on the outcome of Brexit. For personal data held in the United States under Privacy Shield, the Council will also need to confirm that Privacy Shield entries are amended to ensure the UK is covered, as Privacy Shield is an agreement between the EEA and the United States.

Contact the DPO

If you would like to find out more about this annual report, or provide any feedback, please contact the Data Protection Officer.

Phone: 01467 536035
Email: dataprotection@aberdeenshire.gov.uk

In writing to:
Data Protection Officer
Aberdeenshire Council
34 Low Street
Banff
AB45 1AY
Visit: https://aberdeenshire.gov.uk/online/legal-notices/data-protection/

Appendix 1

Data Breaches reported to the ICO:

Breach ID	Description	Outcome
141	Several pages of sensitive personal data (medical details) relating to an eight-year-old child were released in error to a parent who had submitted a Subject Access Request for their own child. This arose due to information having been filed incorrectly by the school – two pupils with same first name. On reviewing the information prior to release, the E&CS Data Protection rep unfortunately did not notice the error.	The DPO proposed a set of recommendations which were accepted by the Service and the ICO. No further action taken by the ICO.
155	A looked after child's box file containing numerous sensitive medical reports, together with the child's passport, birth certificate, photographs, etc. was accidentally dropped on the pavement by a Social Worker, without noticing, while returning the child from a foster care placement. Fortunately, the file was found by a member of the public who quickly thereafter handed the file into the nearest Social Work office.	The DPO proposed a set of recommendations which were accepted by the Service and the ICO. No further action taken by the ICO.
177	A letter containing more information than necessary was sent to all parents of a school advising of a member of staff's suspension. An article subsequently appeared in the press, including a photograph of the member of staff, resulting in actual harm and distress.	The DPO proposed a set of recommendations which were accepted by the Service and which were supplemented by the ICO. No further action taken by the ICO.