Inverclyde council

AGENDA ITEM NO: 10

Report To:	**Policy & Resources Committee**	**Date:**	**21 November 2023**
Report By:	**Head of Legal, Democratic, Digital & Customer Services**	**Report No:**	**LS/111/23**
Contact Officer:	**Vicky Pollock**	**Contact No:**	**01475 712180**
Subject:	**Data Protection Officer Annual Report 2023**		

1.0 PURPOSE AND SUMMARY

1.1 ☐For Decision ☒For Information/Noting

1.2 The purpose of this report is to provide the Policy & Resources Committee with the Data Protection Officer's Annual Report which sets out a note of the Council's data protection performance over the past year, together with the Data Protection Officer's assessment of Inverclyde Council's compliance with data protection legislation.

2.0 RECOMMENDATIONS

2.1 It is recommended that the Policy and Resources Committee notes the Data Protection Officer's Annual Report 2023 as set out at Appendix 1.

Iain Strachan
Head of Legal, Democratic, Digital and Customer Services

3.0 BACKGROUND AND CONTEXT

3.1 Data protection legislation changed significantly with the introduction of the Data Protection Act 2018 on 23 May 2018 and the EU General Data Protection Regulation on 25 May 2018. The UK GDPR, which replicates the EU GDPR into UK law, came into force on 1st January 2021. The data protection legislation increased 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.

3.2 The Data Protection Officer's Annual Report – attached at Appendix 1 – summarises the analysis of the Council's data protection compliance since January 2021. The 2023 report covers the period from 1 January 2023 to 22 October 2023. It is appreciated that this report covers only part of 2023, however, officers undertook in May 2023 to provide a data protection performance report for consideration by the Policy and Resources Committee in 2023. The next annual report, covering the full 2024 period, and the balance of 2023, will be presented to Committee in early 2025.

3.3 In terms of the UK GDPR, there is a requirement that the Data Protection Officer shall report to the highest management level of their organisation. This report fulfils that obligation.

3.4 In 2022 57% of subject access requests (SARs) were responded to within the timescales set by legislation. Although this has improved to date in 2023, sitting at 64.13%, there is a need for further improvement. This level of late responses could result in regulatory action being taken by the regulator, the Information Commissioner (ICO). While there is currently no requirement to submit performance statistics to the ICO, the Council has on request, submitted its 2022 statistics to the ICO. The ICO has responded by stating that ideally, they would like to see a compliance rate of 90% at a minimum. The Council will work with the ICO to improve its SAR compliance rates throughout Council services. It has been noted that there has been a significant increase in the number and complexity of SARs being received by the Council, particularly by the HSCP.

3.5 The number of confirmed data breaches has steadily increased over the past 3 years. This may be due to increased awareness of reporting responsibilities in terms of the Council's established Data Breach Management Protocol. As highlighted in the report, most data breaches are of a minor nature as a result of human error and lack of due care and attention. Services should continue to remind staff of the need to take appropriate care when processing personal data.

3.6 It is critical that all Council staff understand the importance of dealing with the Council's information appropriately, safely and securely. Getting it right means the personal information the Council holds about customers and citizens, and the Council's own information, is protected.
The Information Governance Team is currently developing a training programme for all relevant staff for deliver in late 2023/early 2024. All employees will also be asked to complete refresher training, being completion of the mandatory data protection specific e-learning module.

3.7 In addition to formal training, awareness-raising is also a valuable way of keeping staff appraised of information governance matters. There are various mechanisms available to facilitate this, including: publishing information governance advice and guidance on the Council's intranet, which is updated on a regular basis. The Council's cross-service Information Governance Steering Group meets monthly, and has a standing agenda item on data protection matters, which also helps the sharing of good practice on data protection matters and highlighting of emerging themes and issues.

3.8 It is anticipated that the Data Protection and Digital Information Bill will become law by Easter 2024 or later. This legislation will make a number of material changes to data protection law and updates will be provided to this Committee as required.

3.9 In summary, the Data Protection Officer is of the view that the Council is generally complying with data protection legislation, however there are some areas for improvement which are highlighted above and in the annual report.

4.0 PROPOSALS

4.1 Policy and Resources Committee are asked to note the contents of the Data Protection Officer's Annual Report at Appendix 1.

5.0 IMPLICATIONS

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

SUBJECT	YES	NO
Financial		x
Legal/Risk	x	
Human Resources		x
Strategic (Partnership Plan/Council Plan)	x	
Equalities, Fairer Scotland Duty & Children/Young People's Rights & Wellbeing		x
Environmental & Sustainability		x
Data Protection	x	

5.2 **Finance**

There are no financial implications arising from this report.

One off Costs

Cost Centre	Budget Heading	Budget Years	Proposed Spend this Report	Virement From	Other Comments
N/A					

Annually Recurring Costs/ (Savings)

Cost Centre	Budget Heading	With Effect from	Annual Net Impact	Virement From (If Applicable)	Other Comments
N/A					

5.3 **Legal/Risk**

Article 39 of the UK GDPR sets out the tasks of the DPO. The Council, not the DPO, is responsible for implementing appropriate technical and organisational measures to ensure that it is in compliance with the UK GDPR (Articles 24 and 28). The Council risks regulatory action from the Information Commissioner's Officer if it fails to comply with its obligations under data protection legislation

5.4 **Human Resources**

There are no human resource implications arising from this report.

5.5 **Strategic**

This report will help deliver the outcomes in the Council Plan Theme 3 – Performance - high quality and innovative services are provided giving value for money.

5.8 **Data Protection**

The data protection implications are as highlighted throughout this report and its appendix.

Has a Data Protection Impact Assessment been carried out?

	YES – This report involves data processing which may result in a high risk to the rights and freedoms of individuals.
X	NO – Assessed as not relevant as this report does not involve data processing which may result in a high risk to the rights and freedoms of individuals.

6.0 CONSULTATION

6.1 The Corporate Management Team has been consulted on this report.

7.0 BACKGROUND PAPERS

7.1 None.

Appendix 1

DATA PROTECTION OFFICER'S ANNUAL REPORT 2023

Table of Contents

Foreword 3
The Role of the DPO 4
Data Protection Queries and Advice 4
Data Protection Policy 5
Data Protection Awareness 5
Information Rights 5
Data Breaches 7
Data Protection Complaints 9
Data Protection Impact Assessments 9
Privacy Notices 10
Information Asset Registers 10
Working Groups 10
Contact the DPO 11

Foreword

Since January 2021, the provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. In practice, there is little change to the core data protection principles, rights and obligations, which have now been fully embedded into working practices across the Council.

Whilst there has been some good evidence of data protection compliance in general, there are some areas for improvement which the Council should address in order to further improve the level of compliance.

It should be noted that this annual report deals with the Council's data protection performance from 1 January 2023 to 22 October 2023, with comparative full year data from 2021 and 2022.

There is ongoing room for improvement in responding to subject access requests (SARs) as a high number of responses were issued outside of the timescales set by legislation. This level of late responses could result in regulatory action being taken by the regulator, the Information Commissioner (ICO). While there is currently no requirement to submit performance statistics to the ICO, the Council has on request, submitted its 2022 statistics to the ICO. The ICO has responded by stating that ideally, they would like to see a compliance rate of 90% at a minimum. The Council will work with the ICO to improve its SAR compliance rates throughout Council services.

As of October 2023, there has been a decrease in the number of confirmed data breaches reported to the DPO. Most data breaches are of a minor nature resulting from lack of due care when sending emails or hard copies of correspondence. The number of serious data breaches requiring to be reported to the ICO continues to be low.

It is important for the Council to continue to pay sufficient regard to Data Protection not only to ensure individuals' rights are upheld but also due to the fact that the ICO has various enforcement powers, including the power to levy a fine of up to £17,500,000 or up to 4% of annual global turnover, whichever is larger. In June 2022, the ICO set out a revised approach to public sector enforcement which has resulted in an increased use of their wider powers, including warnings, reprimands and enforcement notices, with fines only issued in the most serious of cases. Additionally, the ICO will be working more closely with the public sector to encourage compliance with data protection law and prevent harms before they happen.

It is anticipated that the Data Protection and Digital Information Bill will become law by Easter 2024 or later. This legislation will make a number of material changes to data protection law and updates will be provided to the Council as required.

Vicky Pollock
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 DPO 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 Council must support the DPO in performing their tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations.

Since April 2021, Vicky Pollock has been appointed as the permanent designated DPO as required by Article 37 of the UK GDPR.

Please note that reference to the DPO in this report includes the Information Governance Team.

Data Protection Queries and Advice

One of the key tasks of the DPO is to inform and advise the Council and its services about their obligations to comply with the UK GDPR and other data protection laws. This is a requirement under Article 39 of the UK GDPR.

The DPO receives a wide range of queries on data protection matters. This involves both providing advice, guidance and supporting various internal processes. Advice is provided on intricate aspects of the law supporting Council services in applying data protection in practice. The DPO also assists with various internal data protection practices such as the review of privacy documentation, monitoring of Data Protection Impact Assessments and the Information Asset Register.

Areas on which advice is being provided include:

- Data Sharing Agreements
- Data Processing Agreements
- Understanding the role of the Council as a Data Controller and its implications
- Understanding the role of external agencies as Data Processors and its implications
- Application of the data protection principles
- Understanding the lawful bases for processing personal data
- Data Protection Impact Assessments
- Data protection risks
- Disapplication of the data protection provisions (exemptions)
- Data protection breaches

There has been a good level of engagement from Council services on various data protection issues. Advice is sought from the DPO on data processing at different

stages. The DPO is also a member of the Council's cross-service Information Governance Steering Group meets monthly, and has a standing agenda item on data protection matters, which also helps the sharing of good practice on data protection matters and highlighting of emerging themes and issues.

Data Protection Policy

The Council's Data Protection Policy was reviewed and updated to ensure that it remains relevant and accurate and was approved by the Policy and Resources Committee on 23 May 2023. The policy will be reviewed again in April 2026.

Data Protection Awareness

Data Protection training and awareness has been incorporated into a data protection specific e-learning module which is mandatory for all employees who have access to a computer and process personal data. All employees are also required to undertake regular refresher training. Training continues to be monitored by the Information Governance Steering Group and further training is provided on a needs basis.

Targeted training was provided to those who process SARs on basic procedures and the application of exemptions and redactions in November 2022. A further training programme is being developed for delivery in early 2024.

Information Rights

Under the UK GDPR, individuals have several 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 the Council's Data Protection Policy.

Number of valid requests received during 1 January 2021 to 31 December 2021

Right	Number Received	Number of responses issued on time	Percentage of responses issued on time
Access Requests	55	n/a*	n/a*
Rectification Requests	1	1	100%
Erasure Requests	1	1	100%
Restriction of Processing Request	0	0	n/a
Data Portability Request	0	0	n/a

*Information not recorded until 2022 once Workpro implemented.

Number of valid requests received during 1 January 2022 to 31 December 2022

Right	Number Received	Number of responses issued on time	Percentage of responses issued on time
Access Requests	82	47	57%
Rectification Requests	1	1	100%
Erasure Requests	1	1	100%
Restriction of Processing Request	0	0	n/a
Data Portability Request	0	0	n/a

Number of valid requests received during 1 January 2023 to 22 October 2023

Right	Number Received	Number of responses issued on time	Percentage of responses issued on time
Access Requests	92	59**	64.13%**
Rectification Requests	0	0	n/a
Erasure Requests	0	0	n/a
Restriction of Processing Request	5	0	n/a
Data Portability Request	0	0	n/a

**As of 22 October 2023, 17 requests were still in progress with time left to respond to them on time. 20 requests have been responded to late, with 4 having been carried over from the previous reporting period.

Although the performance in 2023 to date has improved, the percentage of SAR responses issued on time is too low and there is room for improvement. Services must take action to address late SAR responses, which actions should include having appropriate resources in place to meet statutory timescales. Given the interest in the Council's SAR statistics from the ICO and their comments that they expect a 90% SAR compliance rate, an action plan will be put in place to address compliance levels.

There is a noticeable increase in the number of SARs being submitted to the Council. While most services are seeing the usual level of SARs, the HSCP has seen a large increase in the number, size and complexity of SARs being received. It is not possible to quantify how many requests received relate to the Financial Redress Scheme or the Scottish Child Abuse Inquiry. The purpose of individual requests is not recorded as this is not always provided by requestors. However, evidence suggests that the nature of the SARs being received by the HSCP relate to historic social work involvement and complex children and families' cases, so it can be presumed that the requirements of the Financial Redress Scheme and the Scottish Child Abuse Inquiry are having an impact. This is an impact which is being felt by all Scottish Local Authorities who are seeing a large increase in the number of SARs being submitted.

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. These requests are mainly from Police Scotland who are usually seeking information 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 increased in the past year. This may be due to more accurate recording of requests received. Services are reminded that if they receive such a request, it should be passed to the DPO to be logged.

Number of valid Schedule 2 requests received by year

Year	**Number of requests received**
2021	3
2022	4
1 January to 22 October 2023	6

Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

The Council has in place a Data Breach Management Protocol which has been fully embedded into the Council's data protection processes and procedures.

The ICO will only be notified of a breach when it is deemed to be a 'risk' to the rights and freedoms of affected individuals. Breaches which need to be reported must be reported without undue delay, but not later than 72 hours after becoming aware of it. The obligation to notify the affected data subject only arises when the breach is deemed to be a 'high risk' to the rights and freedoms of affected individuals. The affected data subject(s) should be informed without undue delay.

Number of confirmed data breaches reported by year

Year	Number of confirmed data breaches
2021	21
2022	36
1 January to 22 October 2023	28

Almost all data breaches are as a result of human error and lack of due care and attention. Employee error and disclosure in error account for 89% of confirmed data breaches so far in 2023.

Data breaches by breach type

Data Breach by Type	No. of confirmed breaches 2021	No. of confirmed breaches 2022	No. of confirmed breaches 2023
Employee Error	17	18	11
Loss of Equipment	0	1	2
Confidentiality Breach/Deliberate Misuse	2	1	1
Theft of Data (Physical Equipment, Papers etc.)	0	0	0
Loss of Data	0	0	0
Technical Fault	0	0	0
Disclosure In Error	2	16	14

Data breaches arising by service:

Service Area	2021	2022	1 Jan to 22 Oct 2023
Culture & Communities	1	0	0
Education	8	19	9
Environmental Services	0	0	0
Public Protection	2	3	1
Finance	4	3	2
Legal & Democratic Services	2	2	6
Organisational Development, Policy & Communications	0	0	3
Regeneration & Planning	0	0	0
HSCP - Health & Community Services	1	5	4
HSCP - Children's Services & Criminal Justice	1	2	2
HSCP - Strategy & Support Services	0	1	1
HSCP - Health Addictions and Homelessness	2	1	0
HSCP	0	0	0

While the number has decreased in 2023, approximately 32% of breaches have occurred within Education Services. While this figure is higher in comparison with other services, the figure is proportionate as the service processes personal data at a larger scale in comparison to other services and taking into account the number of education establishments. The DPO has noted that Education Services are pro-active in following the Data Breach Management Protocol and reporting breaches as soon as they become aware. It is also noted that Education Services are training their staff on a regular basis on how to recognise and report a data breach – for example annual training for teachers. This has resulted in a decrease in the number of data breaches being reported by Education Services in 2023.

Almost all data breaches fall below the threshold for reporting to the ICO. In 2022, only one data breach was deemed by the DPO to require reporting to the ICO. No further action was taken by the ICO. So far, in 2023, no breaches have met the threshold for ICO reporting.

Services should continue to remind staff, on an ongoing basis, of the need to take appropriate care when processing personal data – including sending emails and hard copy correspondence.

Data Protection Complaints

The DPO deals with data protection complaints from individuals regarding the Council's data protection practices, which mostly relate to the Council's handling of SAR requests.

Number of formal complaints received by the DPO

Year	Number of complaints received
2021	2
2022	7
1 January to 22 October 2023	5

It should be noted that no complaints have been received from the ICO in any of the years specified in respect of the Council's data protection practices.

Data Protection Impact Assessments

The GDPR introduced a 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.

Number of DPIAs completed

	2021	2022	1 Jan-22 Oct 2023
DPIAs completed	20	24	11

All services must continue to ensure that DPIAs are undertaken as necessary in terms of the Council's established DPIA guidance.

Privacy Notices

A privacy notice is a document which must be provided to individuals to explain how their personal data is processed.
It has two aims:

- to promote transparency; and
- to give individuals more control over the way their data is collected and used.

Transparency is a key principle of the UK GDPR, as it prevents organisations from processing personal data without data subjects' knowledge or approval.

When personal data is being collected directly from data subjects, it is a legal obligation to provide a privacy notice at the time of collection from the data subject.

The Council has a suite of privacy notices for all service areas which are regularly reviewed and updated, the last review having taken place in 2023.

Information Asset Registers

The Council holds a corporate information asset register (IAR) that records assets, systems and applications used for processing or storing personal data across the organisation. The IAR holds details of all information assets, including asset owners, asset location, retention periods and security measures deployed.

The Council is required to review its IAR periodically to ensure that it is kept up to date and accurate at all times.

An annual review is progressed each year, with each service area asked to review and update the assets they hold.

Working Groups

The DPO continues to be 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 a very useful group which discusses matters of shared concern and which is also used to share knowledge and experience so that all 32 Scottish Local Authorities are consistent in their approach to data protection matters.

Information Governance Steering Group – the Head of Legal, Democratic, Digital and Customer Services chairs this internal group which includes representatives from all Council services. The overall purpose of the group is:

- To support and drive the broader information governance agenda across the Council
- To ensure the effective management of all information governance risks
- To provide assurance to the Corporate Management Team (CMT) that appropriate frameworks, workstreams and initiatives are in place to support, co-ordinate, promote, monitor and assure the development and delivery of effective information governance

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: 01475 712180
Email: dataprotection@inverclyde.gov.uk
In writing to:
Data Protection Officer
Municipal Buildings
Clyde Square
Greenock
PA15 1LX
Visit: Data Protection and Freedom of Information - Inverclyde Council