Inverclyde council

AGENDA ITEM NO: 15

Report To:	**Policy & Resources Committee**	**Date:**	**26 March 2019**
Report By:	**Head of Legal & Property Services**	**Report No:**	**LP/043/19**
Contact Officer:	**Andrew Greer**	**Contact No:**	**01475 712498**
Subject:	**Data Protection Impact Assessment Guidance and Template**		

1.0 PURPOSE

1.1 The purpose of this report is to provide the Policy & Resources Committee with an overview of the Data Protection Impact Assessment Guidance and Template (DPIA) (**Appendix 1**) and to seek the Committee's approval of this policy.

2.0 SUMMARY

2.1 The General Data Protection Regulation (GDPR) came into effect on 25 May 2018.

2.2 Article 35 of the GDPR introduces Data Protection Impact Assessments (DPIAs). A DPIA is a legal requirement where the processing may result in a high risk to the rights and freedoms of individuals.

2.3 Therefore, the Information Governance Team has developed DPIA Guidance and Template (**Appendix 1**) in order to assist the Council to comply with this legal obligation under GDPR.

2.4 The GDPR Implementation Group, Extended Management Team and the Corporate Management Team have been consulted regarding this policy and their input has been incorporated into the Guidance.

3.0 RECOMMENDATIONS

That the Committee

3.1 Considers the content of this report; and

3.2 Approves the Council's DPIA Guidance and Template.

Gerard Malone
Head of Legal & Property Services

4.0 BACKGROUND

4.1 The General Data Protection Regulation (GDPR) came into effect on 25 May 2018. Article 35 of the GDPR introduces Data Protection Impact Assessments (DPIAs).

4.2 A DPIA is a legal requirement for any type of processing, including certain specified types of processing, that is likely to result in a high risk to the rights and freedoms of individuals, for example, the introduction of a new CCTV system; open floor working environment; a new IT system for HSCP. Therefore, the Information Governance Team has developed the DPIA Guidance and Template (**Appendix 1)** which will assist the Council meet this legal obligation.

4.3 DPIAs will help the Council identify, assess and mitigate or minimise privacy risks with data processing activities. DPIAs are also particularly relevant when a new project, plan, data processing process, system or technology is being introduced.

4.4 DPIAs will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly. They do not have to eradicate all risks, but should help the Council to minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what the Council wants to achieve. DPIAs support the accountability principle of the GDPR. They will help the Council demonstrate that appropriate measures have been taken to ensure compliance.

4.5 Failure to adequately conduct a DPIA where appropriate is a breach of the GDPR and could lead to substantial fines.

4.6 The Committee Report Template will be amended to reflect DPIA. Officers will indicate in their reports when a DPIA has been completed and attach a copy of the report for reference.

4.7 Training has been delivered to key contacts within Services. This took place on 28 September 2018 and 16 January 2019.

4.8 The GDPR Implementation Group, the Extended Management Team and the Corporate Management Team have been consulted and their feedback has been incorporated into the Guidance.

4.9 The DPIA Guidance and Template is in draft form and Policy & Resources Committee approval is required.

5.0 IMPLICATIONS

5.1 **Finance**

Financial Implications:

One off Costs

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

Annually Recurring Costs/ (Savings)

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

5.2 **Legal**

The Council requires to take the steps as identified in this report to comply with the General Data Protection Regulation.

5.3 **Human Resources**

There are no direct HR implications on this report.

5.4 **Equalities**

There is no direct effect upon equalities within this report.

(a) Has an Equality Impact Assessment been carried out?

	YES (see attached appendix)
X	NO – This report does not introduce a new policy, function or strategy or recommend a substantive change to an existing policy, function or strategy. Therefore, no Equality Impact Assessment is required

(b) Fairer Scotland Duty

If this report affects or proposes any major strategic decision:-

Has there been active consideration of how this report's recommendations reduce inequalities of outcome?

	YES – A written statement showing how this report's recommendations reduce inequalities of outcome caused by socio-economic disadvantage has been completed.
X	NO

5.5 **Repopulation**

There is no implication for repopulation within Inverclyde.

6.0 BACKGROUND PAPERS

6.1 ICO's guidance "Preparing for the Data Protection Regulation – 12 steps to take now" – https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Appendix 1

Information Governance and Management Framework

Data Protection Impact Assessment (DPIA) Guidance

Version 1.0

Produced by:
Information Governance Team
Inverclyde Council
Municipal Buildings
GREENOCK
PA15 1LX

July 2018

INVERCLYDE COUNCIL IS AN EQUAL OPPORTUNITIES EMPLOYER
THIS POLICY BOOKLET IS AVAILABLE ON REQUEST, IN LARGE PRINT, BRAILLE, ON AUDIOTAPE, OR COMPUTER DISC.

DOCUMENT CONTROL

Document Responsibility		
Name	**Title**	**Service**
Data Protection Officer	Data Protection Impact Assessment (DPIA) Guidance	Legal and Property Services

Change History		
Version	**Date**	**Comments**
1.0	July 2018	Draft Guidance
1.2	March 2019	Changes made following consultation period.

Distribution		
Name/ Title	**Date**	**Comments**
GDPR Implementation Group	August 2018	Minor amendments
EMT and CMT	February 2019	Minor amendments

Distribution may be made to others on request

Policy Review		
Review Date	**Person Responsible**	**Service**
March 2020	Information Governance Team	Legal and Property Services

CONTENTS

1. What is a DPIA?

Data protection impact assessments (DPIAs) will help the Council identify, assess and mitigate or minimise privacy risks with data processing activities. DPIAs are mandatory where the processing may result i**n a high risk to the rights and freedoms of individuals.** DPIAs are also particularly relevant when a new project, plan, data processing process, system or technology is being introduced.

The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

They do not have to eradicate all risks, but should help the Council to minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

2. What do we need to be aware of before completing a DPIA?

In order to carry out an effective DPIA, it would assist if you have:

1) Read the GDPR Employee Guide
2) Completed the GDPR e-learning module on Brightwave
3) Read the Information Sharing Protocol
4) Read the Data Protection Policy.
5) Read and understood this guidance and completed any training/e-learning course once available.

3. Why do we need to carry out a DPIA?

DPIAs support the accountability principle of the General Data Protection Regulation (GDPR). They will help the Council demonstrate that appropriate measures have been taken to ensure compliance.

A DPIA is a legal requirement for any type of processing, including certain specified types of processing, that is likely to result **in a high risk to the rights and freedoms of individuals**.

Failure to adequately conduct a DPIA where appropriate is a breach of the GDPR and could lead to substantial fines.

A DPIA will also assist in:

- Identifying and managing risks at an early stage;
- Avoiding unnecessary costs;
- Avoiding inadequate solutions;
- Avoiding enforcement action by the data subjects and/or the Information Commissioner;
- Avoiding loss of trust and reputation;
- Meeting the legal requirements in relation to privacy and reassuring the public that the Council have complied with the legislation;
- Improve transparency and make it easier for the public to understand how and why their information is being used;
- In some cases, it allows the individual to have an input.

4. When do we need to carry out a DPIA?

A DPIA must be carried before any type of processing personal data which is likely to result in a high risk to the rights and freedoms of individuals.

Answering the screening questions in Appendix 1 of this document should help you identify the need for a DPIA at an early stage of your project, which can then be built into your project management or other business process.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

5. Who should carry out a DPIA?

It is the responsibility of the Service which holds the relevant information and is proposing the new use of the personal data or the changes to an existing processing system to carry out a DPIA.

The Council's DPO is prohibited under GDPR to complete the DPIA as this would be a conflict of interest. However, the DPO can assist and must be consulted.

6. Process for DPIA

Step 1: How do we decide whether to do a DPIA?

- Answer the screening questions in Appendix 1 to identify a proposal's potential impact on privacy.
- Begin to think about how project management activity can address privacy issues.
- Start discussing privacy issues with stakeholders.
- If you have any major project which involves the use of personal data it is good practice to carry out a DPIA.

If you carry out this screening exercise and decide that you do not need to do a DPIA, you should document your decision and the reasons for it, including your DPO's advice.

Step 2: How do we describe the processing?

- Explain how information will be obtained, used and retained – there may be several options to consider. This step can be based on, or form part of, a wider project plan.
- This process can help to identify potential 'function creep' – unforeseen or unintended uses of the data (for example data sharing).

Step 3: Consultation Process

- You should seek the views of individuals unless there is a good reason not to.
- If you don't seek views of the individuals, then you must record why you didn't.

- If you use a data processor, you may need to ask them for information and assistance. Your contracts with processors should require them to assist.
- You should consult all relevant and internal stakeholders.
- You may wish to consult ICT, Legal & Property Services and the Information Governance Team.
- A decision on whether you may wish to consult the ICO can be determined at the end of the process.

Step 4: Assessing necessity and proportionality

- Do your plans help to achieve your purpose?
- Is there any other reasonable way to achieve the same result?

Step 5: How do we identify and assess risks?

- Record the risks to individuals, including possible intrusions on privacy where appropriate.
- Assess the corporate risks, including regulatory action, reputational damage and loss of public trust.
- Conduct a compliance check against GDPR and other relevant legislation.
- Maintain a record of the identified risks.

Consider whether the processing could possibly contribute to:

- Inability to exercise rights;
- Inability to access services or opportunities;
- Loss of control over the use of personal data;
- Discrimination;
- Identity theft or fraud;
- Financial loss;
- Reputational damage;
- Physical harm;
- Loss of confidentiality;

- Re-identification of pseudonymised data; or
- Any other significant economic or social disadvantage.

Step 6: How do we identify mitigating measures?

- Devise ways to reduce or eliminate privacy risks.
- Assess the costs and benefits of each approach, looking at the impact on privacy and the effect on the project outcomes.

In reducing risks, you may wish to consider:

- Deciding not to collect certain types of data;
- Reducing the scope of the processing;
- Reducing retention periods;
- Taking additional technological security measures;
- Training to staff to ensure risks are anticipated and managed;
- Anonymising or pseudonymising data where possible;
- Writing internal guidance or processes to avoid risks;
- Using a different technology;
- Putting clear data sharing agreements into place;

Step 7: How do we conclude our DPIA?

- The DPO must be consulted and give a summary of their advice.
- The relevant Head of Service must sign the DPIA.
- Attach all relevant documents used in completing DPIA.
- Consult the ICO if there is still a high risk which cannot be mitigated.

7. What do we do once a DPIA has been completed?

Ensure that the steps recommended by the DPIA are implemented.

Continue to use the DPIA throughout the project lifecycle when appropriate.

All signed DPIAs, must be copied to the DPO who will arrange for them to be recorded in the Register of Completed DPIAs. You must also ensure that the Service Information Asset Register is updated where appropriate, eg, where there is new information asset.

Further advice and assistance

The ICO has published guidance at - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

The Council's Data Protection Officer is Andrew Greer and can be contacted at andrew.greer@inverclyde.gov.uk or by telephone on 01475 712498.

The Information Governance and Complaints Officer is Carol Craig McDonald and can be contacted carol.craig-mcdonald@inverclyde.gov.uk or by telephone on 01475 712725.

Appendix 1

Data Protection Impact Assessment Screening Questions

The GDPR states that the Council must carry out a DPIA if it plans to:

- Systematically monitor a public place on a large scale by for example, installing CCTV cameras;
- Use new technologies, process biometric data (eg fingerprints, facial recognition, retinal scans) and geometric data (an individual's gene sequence);
- Process sensitive personal data or criminal offence data on a large scale;
- Use systematic and extensive profiling with significant effects;
- Match data or combine data sets from different sources;
- Process personal data without providing a privacy notice directly to an individual;
- Profile children or target services at them;
- Process personal data that might endanger an individual's health or safety in the event of a security breach.

The following questions will help you decide whether a DPIA is necessary. Answering "yes" to any of these questions is an indication that a DPIA would be a useful exercise. It will ultimately be for the Service to decide whether a DPIA is required, however, if you are uncertain, then the Information Governance Team can offer assistance.

Please tick all that apply.

□ Will the proposed processing operation involve the collection of new information about individuals?

□ Will the proposed processing operation compel individuals to provide information about them?

□ Will information about individuals be disclosed, as part of the proposal, to organisations or people who have not previously had routine access to the information?

- □ As part of the proposal, are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

- □ Does part of the proposed processing operation involve using new technology which might be perceived as being privacy intrusive? For example, the use of technology that would make the gathering of information about a person easier to find and gather together (particular where moving from paper records to searchable electronic systems) and the use of biometrics or facial recognition.

- □ Will the processing operation result in you making decisions or taking action against individuals in ways which can have a significant impact upon them?

- □ Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

- □ Will the processing operation require you to contact individuals in ways they may find intrusive?

- □ Does part of the proposed changes to the processing operation involve using new or alternate technology? For example, changing the software supplier and so the software involved in the processing operation?

Appendix 2: Data Protection Impact Assessment Template

Step 1: Identify the need for a DPIA

1.1 Explain briefly what project aims to achieve and what type of processing it involves. Refer to links to other documents, such as a project proposal, where applicable.
1.2 Summarise why you identified the need for a DPIA, or if the decision is not to complete a DPIA document the reasons why.

Step 2: Describe the processing

Describe the nature of the processing:

2.1 How will you collect, use, store and delete data?
2.2 What is the source of the data?
2.3 Will you be sharing data with anyone?
2.4 You might find it useful to refer to a flow diagram or other way of describing data flows.
2.5 What types of processing identified as likely high risk are involved?

Describe the scope of the processing:

2.6 What is the nature of the data, and does it include special category or criminal offence data?
2.7 How much data will you be collecting and using?
2.8 How often?
2.9 How long will you keep it?
2.10 How many individuals are affected?
2.11 What geographical area does it cover?

Describe the context of the processing: 2.12 What is the nature of Inverclyde Council's relationship with the individuals? 2.13 How much control will they have? 2.14 Would they expect you to use their data in this way? 2.15 Do they include children or other vulnerable groups? 2.16 Are there prior concerns over this type of processing or security flaws? 2.17 Is it novel in any way? 2.18 What is the current state of technology in this area? 2.19 Are there any current issues of public concern that you should factor in? 2.20 Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: 2.21 What do you want to achieve? 2.22 What is the intended effect on individuals? 2.23 What are the benefits of the processing – for Inverclyde Council, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: 3.1 Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. 3.2 Who else do you need to involve within Inverclyde Council? 3.3 Do you need to ask our processors to assist? 3.4 Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: 4.1 What is the lawful basis for processing? 4.2 Does the processing actually achieve the purpose? 4.3 Is there another way to achieve the same outcome? 4.4 How will you prevent function creep? 4.5 How will you ensure data quality and data minimisation? 4.6 What information will you give individuals? 4.7 How will you help to support their rights? 4.8 What measures do you take to ensure processors comply? 4.9 How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** (Remote, possible or probable)	**Severity of harm** (Minimal, significant or severe)	**Overall risk** (Low, medium or high)

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** (Eliminated reduced accepted)	**Residual risk** (Low medium high)	**Measure approved** (Yes/no)

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Summary of Consultation:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 3: Checklist

This section sets down the matters that you must include in relation to the undertaking of a data protection impact assessment in relation to this principle. Once you have completed the actions, you can tick the appropriate box to show that you have done so. Answering these questions during the DPIA process will help identify where there is a risk that the project will fail to comply with GDPR.

1st Principle: The lawfulness, fairness and transparency principle
☐ Have you identified all of the personal data or special category data involved in the project?
☐ Have you identified all of the uses of the information involved, bearing in mind that there could be a number of uses for the same information – this includes the sharing of or giving access to any personal data or special category data?
☐ Have you identified the purpose of the project?
☐ How will individuals be told about the use of their personal data?
☐ Do you need to amend your privacy notices?
☐ Have you established which conditions for processing apply?
☐ If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
☐ Have you identified the social need and aims of the project?
☐ Are your actions a proportionate response to the social need?
2nd Principle: The purpose limitation principle
☐ Does your project plan cover all of the purposes for processing personal data?
☐ Have potential new purposes been identified as the scope of the project expands?
3rd Principle: The data minimisation principle
☐ Have you assessed whether the personal data or special category data is adequate for the purposes for which it is intended to be used?
☐ Have you recorded how this assessment was done and what were the conclusions and how were they reached? ☐ Have you assessed whether the personal data or special category data is relevant for the purposes for which it is intended to be used?
☐ Have you recorded how this assessment was done and what were the conclusions and how were they reached?
4th Principle: The accuracy principle
☐ Have you ensured that the processing operation includes measures to ensure personal data or special category data remains accurate after the project has been implemented (NB: it is the Council's responsibility to ensure accuracy, this cannot be passed to the data subjects concerned to do so)?
☐ Have you ensured that the processing operation allows you to deal with a request in

connection with the right of rectification?
☐ Have you ensured that the processing operation allows you to deal with the right to restrict processing if exercised?
☐ Have you ensured that the processing operation allows you to correct data which is inaccurate?
☐ Have you ensured that the processing operation allows you to record where the data subject has complained about information being inaccurate but which is not being changed by the Council?
☐ Have you ensured that the processing operation includes steps that will allow you to keep records accurate if stored in a number of different locations?
5th Principle: The storage limitation principle
☐ What retention periods are suitable for the personal data you will be processing?
☐ Are you procuring software which will allow you to delete information in line with the Council's retention periods?
6th Principle: The integrity and confidentiality principle
☐ Do any new systems provide protection against the security risks you have identified?
☐ What training and instructions are necessary to ensure that staff know how to operate a new system securely?