Data Protection Impact Assessment (DPIA) procedure

Procedure Title:	**Data Protection Impact Assessments – all staff**
Purpose:	This procedure explains when a Data Protection Impact Assessment should be completed, the process for doing so, and the resources available to help.
Prepared By:	Information Manager
Original Authorisation:	Data Protection Officer
Version:	2.0
Last reviewed	13/02/2024
Review Cycle	Review annually and re-issue if required
Review Date	February 2025

Contents

1. Introduction

The Council routinely collects, processes, and shares personal information to provide services to customers and service users. When we do so, we are obliged to comply with the data protection principles to ensure that personal data is processed lawfully and appropriately protected. Failure to safeguard personal data will result in reputational, and potentially financial, damage to the organisation.

A Data Protection Impact Assessment (DPIA) provides evidence that an organisation has considered all the data protection principles when designing a process, and has understood, recorded, and mitigated any risks associated with processing personal data in the way proposed. A DPIA is a consultative document and should be considered throughout the design of a system or process. All stakeholders should be involved in a DPIA including, but not limited to, the service proposing the change, the Operational Information Asset Owner (OIAO), the Strategic Information Asset Owner (SIAO), the Information Management Team (IMT), IT Client Team, CGI Chief Security Officer, service users and, in some cases, the UK Information Commissioner's Office (ICO).

Services are responsible for completing DPIAs, as required, in accordance with this procedure. The Council's Information Management Team (IMT) is responsible for administrating the process and supporting services in complying with the principles set out in the General Data Protection Regulation and the Data Protection Act 2018.

2. Scope

This procedure applies to:

- All Council staff (including temporary staff), contractors, consultants, and volunteers that access and use Council information. This includes Elected Members when working on behalf of the Council (but not in their Party or Constituency roles).
- All personal data created, processed, held, and shared by the Council in all locations and in all formats.

3. Roles and Responsibilities

DPIA Author – is responsible for writing a DPIA in consultation with other relevant stakeholders and for leading work on completing any identified improvement actions following a DPIA Assessment.

Data Protection Officer (DPO) - is responsible for monitoring the Council's compliance with data protection principles and providing advice to Senior Management and Information Asset Owners on data protection issues. They are also the key contact between the Council and the ICO. The Service Director for Corporate Governance is the Council's Data Protection Officer (DPO).

Strategic Information Asset Owner (SIAO) – is responsible for ensuring that all personal data complies with data protection legislation. They should support the completion of DPIAs in accordance with Council policy and are ultimately responsible for authorising whether processing commences and when. Strategic Information Asset Owners are Service Directors.

Operational Information Asset Owners (OIAO) - are responsible for managing information assets and risk at Service Level. They are responsible for ensuring that information risk is managed appropriately within their

area and for providing assurances to the Strategic Information Asset Owner (SIAO). Operational Information Asset Owners are normally the service or Group Managers.

Information Management Team (IMT) – is responsible for providing advice, guidance and training in relation to data protection compliance. The IMT also maintains the Council's DPIA register, and co-ordinates the DPIA assessment process.

IT Client Team/CGI Chief Security Officer – are responsible for providing advice and guidance in relation to information security measures. They will also assist the IMT in assessing DPIAs from a technical security perspective.

Senior Information Risk Owner - has delegated authority through the Corporate Leadership Team with specific responsibility for information risk and mitigation, ensuring that any information threats and breaches are identified, assessed and effectively managed. The Service Director for Corporate Governance is the Council's Senior Information Risk Owner (SIRO).

4. Procedure for completing a DPIA

4.1 When to write a DPIA

A DPIA must be completed when you are introducing or changing a process that involves personal data.

A DPIA provides assurance that personal data is processed in accordance with the data protection principles, and evidences the considerations and steps taken to ensure appropriate controls are in place.

4.2 Who should write a DPIA

It is likely that all parties involved in designing or changing processes which handle personal data will need to contribute to the DPIA process. However, ultimately, it is the responsibility of the service area processing the personal data to ensure that a DPIA is completed prior to processing commencing.

The service area may nominate the most appropriate person to write the DPIA, however they cannot be detached from the process. For example, if a new IT system is being introduced, it may be reasonable for the DPIA to be completed by the project manager because they have the technical knowledge of what is proposed. However, as the service will be responsible for the processing in the longer term, they will need to contribute to the DPIA in relation to how personal data will be managed over time.

4.3 Consultation

When introducing new ways to process personal data, it is important to evidence that we have considered the impact of the processing on individuals.

If the processing is entirely new, or a significant change, it is recommended to seek the views of those who will be impacted by the change in process. This enables the Council to understand whether the processing is reasonable and how individuals might be impacted by it. Consultation exercises can take many forms, and services should consider how best to seek the views of relevant groups when designing the process. Examples

might include (but are not limited to): liaison with relevant stakeholders/partners, focus groups, parent/pupil forums, surveys.

It is also recommended that the Information Management Team is consulted as early as possible in the design process to provide guidance on data protection responsibilities. If the new processing relates to the introduction, or change to, ICT systems or software, it is also recommended to contact the IT Client Team for advice on the security measures to consider.

4.4 How to complete a DPIA

A comprehensive DPIA should include the following in order to comply with the General Data Protection Regulation (GDPR):

- a systematic description of the processing (Article 35 (7) (a))
- an assessment of necessity and proportionality (Article 35 (7) (b))
- an assessment of the risks to the rights and freedoms of individuals are managed (Article 35 (7) (c))
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and compliance with legislation.
- interested parties are involved (Article 35 (2) and Article 35 (9))

For ease of use, the Council's DPIA has been mapped against the data protection principles. These require that:

- We tell people why we need their personal data and what we will do with it.
- We don't do anything with someone's information that they would not reasonably expect.
- We only collect information that we need.
- We collect accurate information and, where necessary, keep it up to date
- We don't keep personal data for longer than we need it.
- We keep personal data secure

The DPIA form is available on the Intranet. Data Protection Impact Assessment Template V2.0.docx (sharepoint.com)The IMT has produced guidance to support authors completing DPIAs, and the form itself also refers to specific documents available to help those completing the form.

Authors should complete the DPIA in as much detail as possible by either providing evidence of the controls in place, or indicating what will be in place prior to the processing commencing.

Once completed, the DPIA must be submitted to the IMT for assessment.

4.5 Receipt of DPIA

Following receipt of the DPIA, this will be logged in the DPIA Register in the SharePoint Site, an acknowledgement email will then be sent to the author/submitter which details; the reference number of the DPIA, when it will be assessed by the IMT in consultation with the IT Client Team and the CGI Chief Security Officer, who will be responsible for completing the Assessment Report.

4.6 DPIA Assessment

The IMT will assess the proposed processing against the data protection principles, taking account of the Security Impact Assessment received from the CGI Chief Security Officer and any comments from the IT Client Team, and in liaison with the Data Protection Officer as necessary. The IMT will provide a report back to the author (normally within two weeks) indicating the level of compliance based on the information provided within the DPIA.

The assessment report will identify any improvement actions which are considered necessary. These could include the creation of privacy notices, provision of further technical information, recording of risks, or documenting of procedures. Improvement actions will be given a priority level so it is clear what action must be taken before the processing is recommended to begin. Appendix B indicates the elements that will be considered as part of the assessment process, and how priority levels are decided upon.

As part of their assessment, the IMT will indicate whether the overall processing is categorised as low, medium, of high-risk processing. Appendix C indicates the factors that will be considered when identifying the risk category of the processing.

DPIAs which relate to High-Risk processing will be referred to the Council's Data Protection Officer (DPO) for comment. In some instances, DPIAs which relate to Medium Risk processing may also be referred to the DPO for comment. Under legislation, DPIAs documenting high risk processing may also need to be referred to the UK Information Commissioner's Office (ICO) prior to the processing commencing [see 4.9 ICO Consultation].

The DPO will determine whether processing should be categorised as high risk.

4.7 Next steps

Following receipt of the DPIA assessment report, the DPIA author/service area should work through any recommended improvement actions. Once completed, the DPIA, the Assessment report, and evidence of completed improvement actions should be submitted to the Operational Information Asset Owner, or if required the Strategic Information Asset Owner, for the processing to be authorised.

Processing must not commence unless authorised by the Operational Information Asset Owner.

4.8 OIAO Authorisation

The Strategic Information Asset Owner (SIAO) is ultimately responsible for how personal data they are responsible for is processed. The SIAO is the Service Director of the Service who owns the personal data being processed. However, the management of this responsibility will normally be delegated to an Operational Information Asset Owner (OIAO), the manager of the service. In most circumstances, it will be appropriate for the OIAO to sign off the DPIA. However, if a process involves personal data from multiple service areas, the DPIA will need to be authorised/agreed by multiple OIAOs.

The OIAO will review the DPIA, the risks identified through the assessment report, and the actions taken to mitigate the risks highlighted, and decide whether they are happy for the processing to commence.

In making this decision, the OIAO should:

- Satisfy themselves that appropriate action has been taken, and can be evidenced, to mitigate any risks identified in the assessment report.
- Consider whether the DPIA should be re-submitted for IMT assessment to provide assurance around mitigation actions (this is particularly recommended if high risks were identified in the first assessment).
- Consult with the DPO and the SIAO if it is considered necessary to commence processing with high priority actions outstanding.

Recommendations are given priority levels to assist OIAOs in assessing the significance of them not being actioned. If an OIAO desires to authorise a DPIA which has outstanding Red Priority recommendations, they must consult with the SIAO and the DPO first.

If the DPIA is categorised as high-risk processing, it must be referred to the DPO prior to the processing commencing. This is to assess whether the DPIA also needs to be referred to the ICO for consultation.

4.9 ICO Consultation

Where processing has been classified as high risk (see Appendix C), the DPIA may need to be referred to the ICO for consultation. Data protection legislation requires DPIAs to be referred to the regulator when the risks associated with the processing are still considered to be high, despite mitigation actions.

When a DPIA is identified as high risk, the SIAO should send the DPIA, Assessment Report, and evidence of actions to the DPO who will assess whether risks have been sufficiently mitigated, or whether referral to the ICO is necessary.

If referral is required, the DPO will arrange this. Under data protection legislation, the ICO can take up to 14 weeks to provide a view on a DPIA submitted to them and processing should not commence until their view is known.

4.10 Record-keeping

The service should maintain a record of the DPIA, and all supporting documentation, for the period that the processing is operational in accordance with the documented Record Retention Schedule in the Information Asset Register. This enables the Council to answer any concerns from data subjects, or the ICO, in relation to the processing. Relevant records to evidence the DPIA process will include:

- DPIA Form
- DPIA Assessment Report
- Evidence of actions taken against report recommendations
- IAO authorisation
- Record of DPO consultation
- Correspondence with ICO
- Record of when processing commenced.

Additionally, copies of authorised DPIAs should be sent to the IMT with confirmation of when the processing is due to commence. The DPIA will be included on the Council's DPIA register. Services should also notify the IMT when a processing activity ceases.

4.11 Assurance monitoring

To provide assurance that the DPIA process is managing and mitigating risks associated with personal data processing effectively, the IMT will conduct a programme of monitoring compliance with DPIA improvement actions.

DPIAs relating to high-risk processing will be monitored by the DPO as part of the authorisation process. In addition, the IMT will assure compliance with improvement actions for a sample of Low and Medium risk DPIAs.

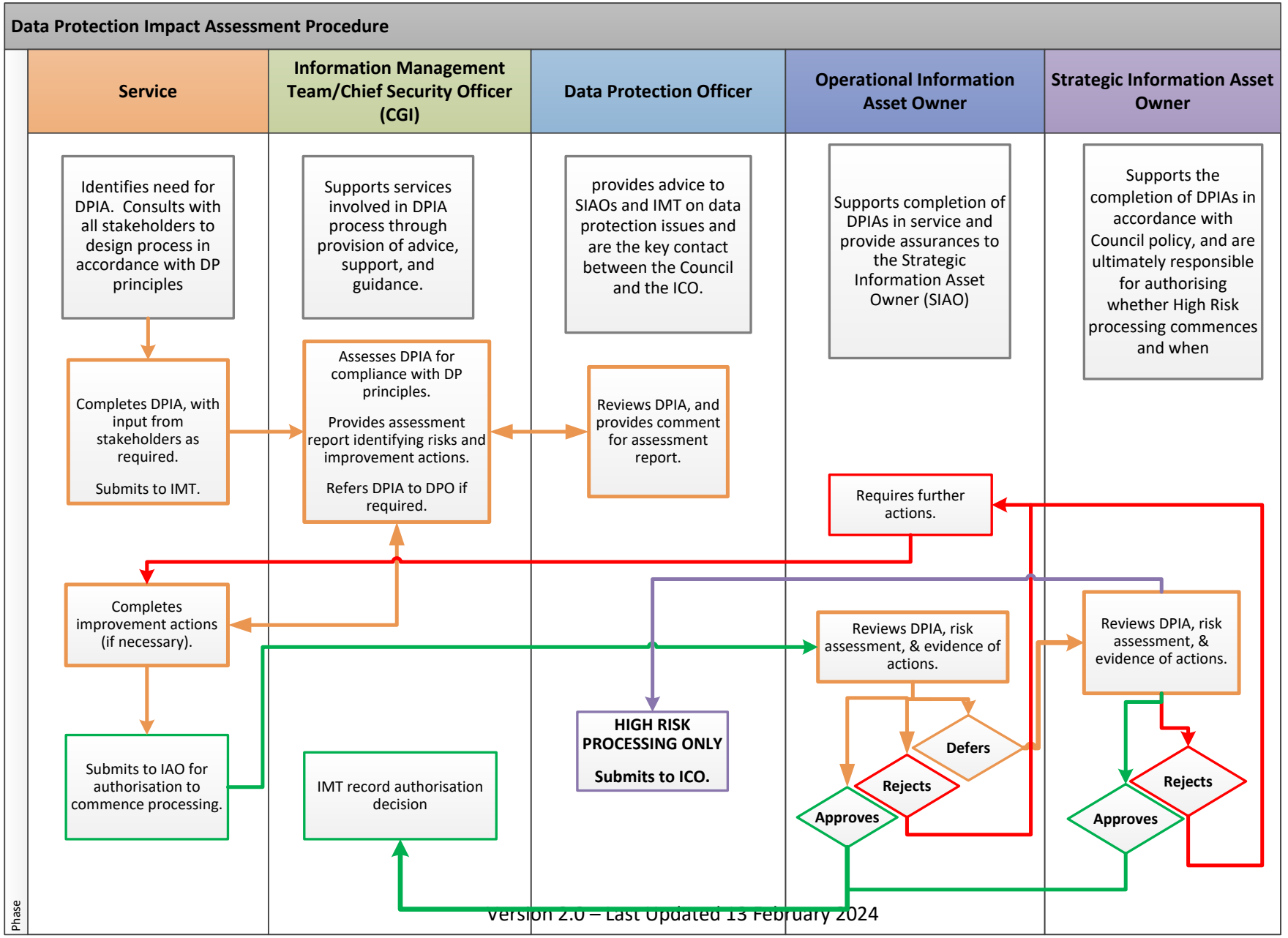
When a DPIA has been identified for assurance, the IMT will contact the DPIA author and request evidence of progress against the improvement actions highlighted in the DPIA assessment report. If risks are identified as part of this assurance process, they will be reported to the OIAO.

5. Related documents

All relevant documentation listed below can be found on the Information Management page on the intranet.
Writing a DPIA Guide and Checklist.
Data Protection Impact Assessment Template
SCARRS
Third Party Assurance Form

6. Further information and contact details:

Information Management Team via email at : dataprotection@scotborders.gov.uk


Data Protection Impact Assessment Procedure
Service
Information Management Team/Chief Security Officer (CGI)
Data Protection Officer
Operational Information Asset Owner
Strategic Information Asset Owner
Identifies need for DPIA. Consults with all stakeholders to design process in accordance with DP principles
Supports services involved in DPIA process through provision of advice, support, and guidance.
provides advice to SIAOs and IMT on data protection issues and are the key contact between the Council and the ICO.
Supports completion of DPIAs in service and provide assurances to the Strategic Information Asset Owner (SIAO)
Supports the completion of DPIAs in accordance with Council policy, and are ultimately responsible for authorising whether High Risk processing commences and when
Completes DPIA, with input from stakeholders as required.
Submits to IMT.
Assesses DPIA for compliance with DP principles.
Provides assessment report identifying risks and improvement actions.
Refers DPIA to DPO if required.
Reviews DPIA, and provides comment for assessment report.
Requires further actions.
Completes improvement actions (if necessary).
Reviews DPIA, risk assessment, & evidence of actions.
Reviews DPIA, risk assessment, & evidence of actions.
HIGH RISK PROCESSING ONLY
Submits to ICO.
Defers
Rejects
Approves
Rejects
Approves
Submits to IAO for authorisation to commence processing.
IMT record authorisation decision
Phase

Appendix A – Glossary of Terms

Data controller – is the organisation which is responsible for deciding how personal data is processed. The Council will normally be the Data Controller in relation to processing carried out by service areas, however, depending on the circumstances there may also be other data controllers e.g. partnership working may require arrangements to be made between multiple organisations/data controllers.

Data processor – is an organisation/individual responsible for processing personal data on the Council's behalf. System providers, contractors, third party organisations might be considered data processors if they handle/store personal data for the Council.

Data protection principles – These provide the framework of how personal data should be processed by an organisation in order to comply with data protection legislation.

Personal data – is any information which identifies a living individual. Name, Address, Date of Birth, email address, Signature, Unique Reference Number (Employee Number, National Insurance Number)

Special category data – is particular types of personal data which are considered to be more sensitive e.g. information about health, religious beliefs, political opinions, trade union membership, sexual orientation, ethnicity, and biometric or genetic data.

Conditions of processing – refer to the lawful reasons which allow an organisation to process personal data.

Data Protection Officer (DPO) - is responsible for monitoring the Council's compliance with data protection principles and providing advice to Senior Management on data protection issues. They are also the key contact between the Council and the ICO.

DPIA – an assessment tool to evidence compliance against the data protection principles. It is Council policy for DPIAs to be completed on all occasions when new processes handling personal data are introduced or changed. It is a mandatory, legal requirement, for organisations to complete a DPIA for all high-risk processing.

High risk processing – is when a process is likely to have a significant impact of the rights and freedoms of individuals, either because it will affect decisions made about individuals or could put them at risk if something goes wrong. The DPO is responsible for deciding whether processing is high risk, examples of the considerations are included in Appendix C.

Strategic Information Asset Owner (SIAO) – is responsible for ensuring that all personal data complies with data protection legislation. They should support the completion of DPIAs in accordance with Council policy and are ultimately responsible for authorising whether processing commences and when. Strategic Information Asset Owners are Service Directors.

Operational Information Asset Owners (OIAO) - are responsible for managing information assets and risk at Service Level. They are responsible for ensuring that information risk is managed appropriately within their

area and for providing assurances to the Strategic Information Asset Owner (SIAO). Operational Information Asset Owners are normally the service or Group Managers.

Information Commissioner's Office (ICO) – is the UK regulator for data protection legislation. They are responsible for advising on data protection compliance, and enforcement.

Information Risk – risks relating to information which could lead to non-compliance with statutory responsibilities and best practice. Like other risks, information risks should be recorded and managed through the Council's risk management framework.

Information Rights – are rights granted to individuals under data protection legislation, and other associated information laws. Under data protection legislation, people have the right to access their personal data, understand why and how it is processed, and, in certain circumstances, to object to or restrict processing, ask for the data to be shared with another data controller, request that decisions are not made about them by automated means only.

Organisational controls – are measures that are taken to protect personal data that the Council processes. These can data protection training, documented procedures, physical security measures, and governance controls such as information sharing agreements and contract clauses.

Privacy notice – this is information provided to data subjects to inform them about why we need their personal data and what we will do with it.

Technical controls – are specifically technical measures which protect personal data held or processed electronically. These are particularly relevant when new systems are being introduced and may include access controls, vulnerability testing, and encryption arrangements.

Register of processing – is a list of all the activities undertaken by the Council which process personal data. The Council's Register of Processing is managed by the IMT.

Retention Schedule – sets out the agreed legal and business rules which govern how long information should be retained by the Council. Retention rules should be applied routinely and consistently to all Council records regardless of their format. Failure to do so should be recorded as an information risk in accordance with the Council's risk management framework.

Senior Information Risk Owner (SIRO) - has delegated authority through the Corporate Leadership Team with specific responsibility for information risk and mitigation, ensuring that any information threats and breaches are identified, assessed and effectively managed.

Appendix B – DPIA Assessment IMT Checklist

Introduction

A DPIA provides evidence of a consultative process which evidences how an organisation has met its obligations under data protection legislation. The Council's DPIA process is based upon completion of the DPIA form, which asks Services to evidence how processing meets the data protection principles. Although the form provides the foundation to a DPIA submission, a number of documents may also be included to evidence of controls which are planned or in place. These might include:

- DPIA form
- Privacy information
- Procedure documentation
- Security documentation
- Information Sharing Agreement / Contract clauses.

Proposed controls should be referred to within the DPIA form. It should be clear whether the controls already exist or are in development.

Assessing a DPIA

A comprehensive DPIA should evidence the following to comply with the requirements of GDPR:

- a systematic description of the processing (Article 35 (7) (a))
- an assessment of necessity and proportionality (Article 35 (7) (b))
- an assessment of the risks to the rights and freedoms of individuals are managed (Article 35 (7) (c))
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and compliance with legislation.
- involvement of interested parties (Article 35 (2) and Article 35 (9))

When assessing a DPIA:

Use the DPIA checklist to identify whether sufficient information has been supplied.

Identify any gaps, and the risks associated with those gaps, within the Assessment report.

Recommend actions which should be taken to mitigate risks and designate a priority level for completion.

Writing an Assessment Report

The Assessment Report should indicate to service areas how compliant their proposed process is with data protection legislation. If there are concerns about the level of compliance, these should be explained and risk assessed so that authors and Information Asset Owners understand how critical the gaps are. The report should indicate recommended actions to improve the process and achieve compliance.

Recommendations should be clearly defined so they can be actioned. If a level of quality assurance or validation is required, this should be stated within the recommendation. Examples of recommendations include:

- Update DPIA to reflect correct processing conditions (Amber priority)
- Complete an information sharing agreement (Red priority)

- Request system vulnerability information from supplier and validate with CGI/IT Client Team (Red priority)
- Document procedures for how personal data will be processed (Red priority)
- Consult with IGU to improve privacy information (Green priority)

Recommendation Priority Levels

Priority levels are defined as:

Red priority	Action must be completed prior to processing commencing. Failure to do so would likely result in a breach of data protection legislation, risking significant financial and reputation damage to the Council. An example of this would be where privacy information has not been evidenced, or insufficient security controls are in place.
Amber priority	Action should be completed before processing commences or shortly thereafter. Failure to complete the action will present a risk to the Council over time, because compliance with data protection legislation cannot be adequately evidenced but is not sufficiently severe to prevent processing commencing. An example of this would be where an incorrect condition of processing has been identified and the DPIA requires updating.
Green priority	Action represents best practice and is recommended but is not required for the processing to be considered lawful. An example of this would be where there is adequate privacy information in place, but suggestions have been made regarding how this might be improved.

Appendix C – Processing Risk Levels

High Risk Processing

Processing will be classified as High Risk if any of the following factors apply.

1. The processing involves **a degree of evaluation or scoring, including profiling and predicting, which will influence decisions made about the individual**. This processing will be particularly sensitive where it concerns aspects of the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements (Recitals 71 and 91).
2. The processing involves **automated decision making with a legal or similar significant effect**. This processing will be particularly sensitive if it could lead to individuals being excluded or suffering discrimination. Automated processing, which will have little or no effect on an individual, should not be considered as meeting this criterion.
3. The processing involves **systematic monitoring** used to observe, monitor or control data subjects, including data collected through networks or publicly accessible areas. This is particularly sensitive where it is likely that a data subject will not be aware of the monitoring and will be unable to take steps to avoid it e.g. public space CCTV.
4. The processing involves **sensitive personal data or data of a highly personal nature**. This will include largescale processing of special category data, as well as personal data relating to criminal convictions or offences. This is particularly sensitive as the impact on a person's rights and freedoms is greater if things go wrong.
5. The processing is **large scale**. The GDPR does not define large scale but the following factors should be considered: (a) the number of data subjects concerned, (b) the volume of data and/or range of different data items being processed; (c) the duration, or permanence, or the processing; (d) the geographical extent of the processing.
6. The processing involves **matching or combining of datasets** from different processing activities, or different data controllers, in a way which would be exceed the reasonable expectations of the data subjects.
7. The processing involves **data concerning vulnerable data subjects**. This is particularly sensitive due to the increased power imbalance between the data subjects and the data controller, meaning individuals may be less able to consent to, or oppose, processing of their data. Vulnerable data subjects may include children, employees, vulnerable adults, or any case where there is an imbalance of power between the data controller and data subject is identified.
8. The processing involves **the innovative use or application of new technological or organisational solutions**. This is particularly sensitive where the new or combined use of data means that the potential impact on individuals cannot be wholly predicted. For example, the "Internet of Things" presents the opportunity to make a great impact on service delivery, but may also have a significant impact on individuals' daily lives and privacy which requires proper assessment.
9. The processing might **prevent data subjects exercising a right or using a service**. This is particularly sensitive where such decisions are made by automated means alone, e.g., if data is screened in order to refuse a person's eligibility for a service or benefit.

High Risk DPIAs should be forwarded to the DPO for comment. The DPO will ultimately decide whether the processing should be categorised as High or Medium Risk.

Medium Risk Processing

Processing will be classified as Medium risk if either of the following apply:

(i) Even with controls in place, there remains a risk that, should things go wrong, individuals could be significantly impacted by the processing.
(ii) A number of controls are missing which would indicate that the processing, as presently planned, will not comply with data protection legislation.

In the case of (i), the DPIA should be referred to the DPO for comment. In the case of (ii), the Assessment Report should include high priority improvement actions which will require to be completed before processing commences. If an OIAO decides that it is necessary to commence processing with high priority actions outstanding, they must consult the SIAO and the DPO first.

Low Risk Processing

Processing will be classified as Low risk if:

The processing complies with data protection principles and controls are in place to provide assurance that it will not result in a significant impact to data subjects' rights and freedoms.

Appendix D – DPIA flow chart