CLEVELAND POLICE

Data Protection Impact Assessment (DPIA)

Policy Number	315
Policy Owner	Head of Information Management
Version	1.3
Last Review Date	09/09/2021
Next Review Date	09/09/2024
Date of approval	October 2018
Protective Marking	Official

This document has been assessed for:	
Compliance with Legislation	☒
Equality Impact Assessment	☒
Freedom of Information issues	☒
Human Rights compliance	☒
Health and Safety	☒
Risk Management	☒

Data Protection Impact Assessment (DPIA) Policy

1. Policy statement

A Data Protection Impact Assessment (DPIA), (previously known as a Privacy Impact Assessment (PIA)), is a process which enables organisations to identify and address the likely privacy impact of new initiatives and projects.

Cleveland Police will use the guidance on DPIAs contained within the College of Policing Authorised Professional Practice (APP) – Information Management – Data Protection. The purpose of this policy is to provide police personnel with guidance in exercising the requirements as set out within the APP and as set out within other guidance such as the Information Commissioner's Office (ICO) 'Data Protection Impact Assessment' guidance.

2. Purpose

Cleveland Police will use as its default decision making process the ICO guidance *Data protection impact assessments* (DPIA) and the College of Policing APP on Information Management Information Sharing and Data Protection and any additional guidance or Code of Practice issued by the ICO as a result of the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018.

The GDPR introduces a new obligation upon a Controller (Chief Constable) to undertake a DPIA before carrying out processing likely to result in high risk to the interests of individuals.

This policy is applicable to all Cleveland Police staff, including police officers, police staff, police community support officers, special constables and volunteers. It includes staff whether they are employed on a full-time, part-time, casual or temporary basis. It also includes non - Cleveland Police staff that have access to Cleveland Police systems and have the use of a Cleveland Police e-mail account.

3. Principles

It is the policy of Cleveland Police to consider and respect the privacy of individuals. This policy and associated DPIA template, guidance and process map have been developed to ensure Cleveland Police's compliance with the:

- Data Protection Act 2018;
- UK General Data Protection Regulation;
- Human Rights Act 1998;
- Common Law Duty of Confidentiality;
- Information Commissioner's Office guidance – Data Protection impact assessments;

- Information Commissioner's Office – Guide to law enforcement processing;
- College of Policing's Authorised Professional Practice – Information Management – Sharing Police Information and Data Protection;
- Article 29 Data Protection Working Party – set up under Article 29 of the EU Directive 95/46/EC – *Guidelines on Data Protection Impact Assessment (DPIA and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.*

The key principles of the policy are:

- The DPIA process will identify risks to the privacy of individuals, assess legislative requirements, such as Data Protection legislation and the Human Rights Act 1998, foresee potential issues and detail/bring forward risk mitigations and solutions whenever new or amended uses of personal data by Cleveland Police are proposed;

- A DPIA is a process which enables organisations to identify and address the likely privacy impact of new initiatives and projects. It covers privacy issues on a wider scale than data protection and information security considerations which should also be undertaken;

- The DPIA process is most effective when conducted at the design stage, when decision-making can be influenced. The aim is to build privacy and legislative considerations into new projects and initiatives, to reduce the need for disruptive and often costly remedial work;

- Cleveland Police will take a privacy by design approach. Such an approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

    - Potential problems are identified at an early stage, when addressing them will often be simpler and less costly;
    - Increased awareness of privacy and data protection across the organisation;
    - Organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act 2018 and the GDPR;
    - Actions are less likely to be privacy intrusive and have a negative impact on individuals.

- The DPIA process will consider compliance risks, and also the broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus will be on the potential for harm – whether physical, material or non-material – to individuals or to society at large. To assess the level of risk the DPIA will consider the likelihood and the severity of any impact on individuals. It will consider the risk based on the specific nature, scope, context and purposes of the processing;

- Consideration will also be made as to whether the processing would lead to a loss of public trust and the impact it will have on society as a whole;

- The GDPR requires that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

4. Powers and Legislation

- Data Protection Act 2018;
- UK General Data Protection Regulation;
- Human Rights Act 1998;
- Common Law Duty of Confidentiality;
- Information Commissioner's Office guidance – Data Protection impact assessments;
- Information Commissioner's Office – Guide to law enforcement processing;
- College of Policing's Authorised Professional Practice – Information Management – Sharing Police Information and Data Protection;
- Article 29 Data Protection Working Party – set up under Article 29 of the EU Directive 95/46/EC – *Guidelines on Data Protection Impact Assessment (DPIA and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.*

5. Policy Detail

Cleveland Police will use the College of Policing Authorised Professional Practice (APP) – Information Management – Data Protection to ensure that statutory obligations are met. In addition, Cleveland Police will take due cognisance to guidance issued by the ICO. Cleveland Police will also take in to account current Data Protection legislation (i.e. Data Protection Act 2018 and GDPR) and any subsequent guidance issued by the ICO or the College of Policing etc. The following process will be adopted.

Cleveland Police will ensure that privacy and data protection is a key consideration in the early stages of any project, initiative or when entering any new data sharing arrangements and then throughout its lifecycle for example when:

- Using new technologies such as building new IT systems for storing or accessing personal data;
- Developing legislation, policy or strategies that have privacy implications such as an impact on privacy through the collection of use of information, or through surveillance or other monitoring;
- Embarking on a data sharing initiative where two or more organisations seek to pool or link sets of personal data;
- A proposal to identify people in a particular group or demographic, and initiate a course of action;
- Using existing data for a new and unexpected or more intrusive purpose;

- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV);
- A new database which consolidates information held by separate parts of an organisation;
- When planning to use systematic and extensive profiling with significant effects;
- When processing special category or criminal offence data on a large scale;
- When systematically monitoring publicly accessible places on a large scale (e.g. CCTV). (This is separate to requirements issued by the Surveillance Camera Commissioner).

The consideration of whether a DPIA is required is particularly important when a new business process or technology initiative involves the collection, recording, sharing or retention of personal information. For a DPIA to be effective it should be applied at a time when it is possible to have an impact on the project.

The undertaking of the DPIA process will assist in ensuring that privacy and data protection issues are considered. The core principles of a DPIA can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals.

Cleveland Police should be in a position to identify the need for a DPIA at an early stage and will look to building this into the project management process and any other relevant business processes. Cleveland Police will integrate core privacy consideration into existing project management and risk management methodologies and policies (Privacy by Design).

A DPIA must be signed off prior to high risk processing commencing.

Under Data Protection legislation Cleveland Police is required to undertake a DPIA for processing of personal data that is likely to result in a high risk to an individual's rights and freedoms. An effective DPIA can also bring broader compliance, financial and reputational benefits; this will assist the Force in demonstrating accountability and will assist in building trust and engagement with individuals. Cleveland Police will always carry out a DPIA if we plan to process personal data that:

- Uses systematic and extensive profiling with significant effects – any systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or similarly significantly affect an individual;
- Use large scale sensitive data - processing on a large scale of special category data or personal data relating to criminal convictions and offences;
- Systematically monitor publicly accessible places on a large scale.

Cleveland Police will consider whether a DPIA should be completed if the processing meets any of the following:

- **Innovative technology**: processing involving the use of innovative technologies, or the unique application of existing technologies (including AI);
- **Denial of service:** decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data;
- **Large-scale profiling**: any profiling of individuals on a large scale;
- **Biometrics:** any processing of biometric data;
- **Genetic data**: any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject;
- **Data matching:** combining, comparing or matching personal data obtained from multiple sources;
- **Invisible processing:** processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 of the GDPR would prove impossible or involve disproportionate effort;
- **Tracking:** processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment;
- **Targeting of children or other vulnerable individuals**: the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if there is an intention to offer online services directly to children;
- **Risk of physical harm:** where the processing is of such a nature that a personal data breach could jeopardise the physical health or safety of individuals.

Even if there is no specific indication of likely high risk, a DPIA will be undertaken for any major new project involving the use of personal data.

It may be possible to justify a decision not to carry out a DPIA if the Information Asset Owner is confident that the processing is nevertheless unlikely to result in a high risk. The reasons for not undertaking a DPIA should be sent to Information Management Unit for recording.

A DPIA should be seen as a live document which should be reviewed periodically by the Information Asset Owners or business area lead, and certainly when any changes to the processing are proposed.

The responsibility for ensuring that a DPIA is undertaken lies with the Information Asset Owner (IAO), this activity can be delegated to the Project Manager or another subject matter expert who will be responsible for ensuring that appropriate consultation has taken place. The IAO will own any residual '*information risks'* upon project or initiative closure. It is imperative that the IAO is identified at the early stage of the project as they will need to have an overview of or involvement in the DPIA process.

There will be a requirement to ensure that at the early stages of any project or initiative that involves the processing of personal data, a DPIA screening questionnaire will be undertaken. The questionnaire will identify whether a DPIA is required. The screening questionnaire will be contained within the DPIA template. A completed screening questionnaire is a pre-requisite that must be attached to all business cases submitted to the Triage Board and any procurement work request. If answering yes to any of the screening questions, you must contact the Data Protection Officer (DPO) or Information Security Team to discuss the DPIA requirements further. If it is decided not to carry out a DPIA the reasons for this will be documented.

The DPIA template can be found on the force intranet:

Templates - All Documents

Data Protection Impact Assessment Template here

Cleveland Police will ensure that the DPIA process will:

- Describe the nature, scope, context and purposes of processing;
- Identify measures that the Force can put in place to eliminate or reduce high risks;
- Record the outcome of the DPIA process, including any difference of opinion with the DPO or individuals consulted;
- Individuals (or their representatives) and other relevant stakeholders will be consulted (as appropriate);
- As part of the DPIA process the Force DPO will be consulted for advice this is a mandatory requirement under the data protection legislation;
- Identify whether the processing is necessary for and proportionate to Force purposes and the DPIA will describe how the Force will ensure data protection compliance;
- An objective assessment of the likelihood and severity of any risks to individual's rights and interests will be undertaken;
- The Force will implement the measures identified and integrate them into the relevant project plan;
- DPIAs will be kept under review and will be revisited if necessary.

The DPIA guidance document and DPIA template identify the process which will be followed. The early stages of the DPIA process will help the Force understand the potential impact on privacy and the steps which may be required to identify and reduce the associated risks. The DPIA does not have to eradicate the risk, but should help to minimise risks and consider whether or not they are justified.

6. Role of the Data Protection Officer

Advice regarding the DPIA process will be sought from the DPO who will provide advice on:

- Whether a DPIA is required;

- How a DPIA should be undertaken;
- Whether to outsource the DPIA or do it in house;
- What measures and safeguards can be undertaken to mitigate risks;
- Whether the DPIA has been undertaken correctly;
- The outcome of the DPIA and whether the processing can go ahead;
- Advice provided by the DPO will be recorded within the DPIA;
- If the DPO's advice is not followed the reasons for not following the advice will be recorded and the decision made must be justified;
- The DPO will monitor the on-going performance of the DPIA, including how well the planned actions to address the risks have been addressed.

When a new project/initiative involving the processing of personal information is being considered the IAO, Project Manager or subject matter expert will contact the DPO to arrange a meeting.

Upon completion of the DPIA template the Project Manager or subject matter expert and IAO will review, sign off and send a copy to the Data Protection Officer. The DPO may seek the views of the Information Security Manager and Records Manager as necessary. The DPIA will then be considered and signed off by the DPO, or escalated to the Senior Information Risk Owner (SIRO) if necessary. The DPO can be contacted for advice at any time during the process. **To reiterate, the processing must not commence until the DPIA has been signed off.**

The outcomes of the DPIA will be integrated back into the project plan (or initiative process). The IAO/Project Manager/subject matter expert will ensure that the steps recommended by the DPIA are implemented. The DPIA will continue to be used throughout the lifecycle of the project or initiative when appropriate. The implementation of privacy solutions will be carried out and recorded. The DPIA will be referred to if the project or initiative is reviewed or expanded in the future.

Consultation will take place with the ICO if any high risks identified as part of the DPIA process cannot be mitigated (this is a legal requirement under data protection legislation). The consultation process will be undertaken by the business area proposing to undertake the initiative - Information Management Unit are a consultee.

Following approval and sign off consideration will be made to publishing the DPIA and providing it is considered suitable for disclosure under the Freedom of Information Act 2000 (FOI), the document may also be published on the Force website. Proactive publication will improve transparency and accountability and will make individuals aware how processing activity affects them. Sensitive information considered exempt under FOI will be redacted.

The DPIA is not a one-off exercise and will be seen as an on-going process and will be kept under regular review by the project manager (during project stage) or Information Asset Owner and business are leads once transitioned to business as usual.

The DPO will maintain a log of all DPIAs carried out in the Force.

The DPIA process will be embedded into Force policies and procedures.

7. Appendices

Appendix	Description
1.	Data Protection Impact Assessment Process

8. Compliance and monitoring

The Head of Information Management is responsible for the accuracy and integrity of this document. This policy will be continuously monitored, and updated when appropriate, to ensure full compliance with legislation.

The Head of Information Management will review this process to ensure that all aspects are being adhered to in accordance with the framework of this policy.

This policy will undergo regular reviews to assess its effectiveness and applicability; this will be planned at least on an annual basis and may be prompted between planned reviews by any significant changes to legislation or national guidance (APP).

9. Version control

This policy will be reviewed and updated at least every three years by the owner, and more frequently if necessary.

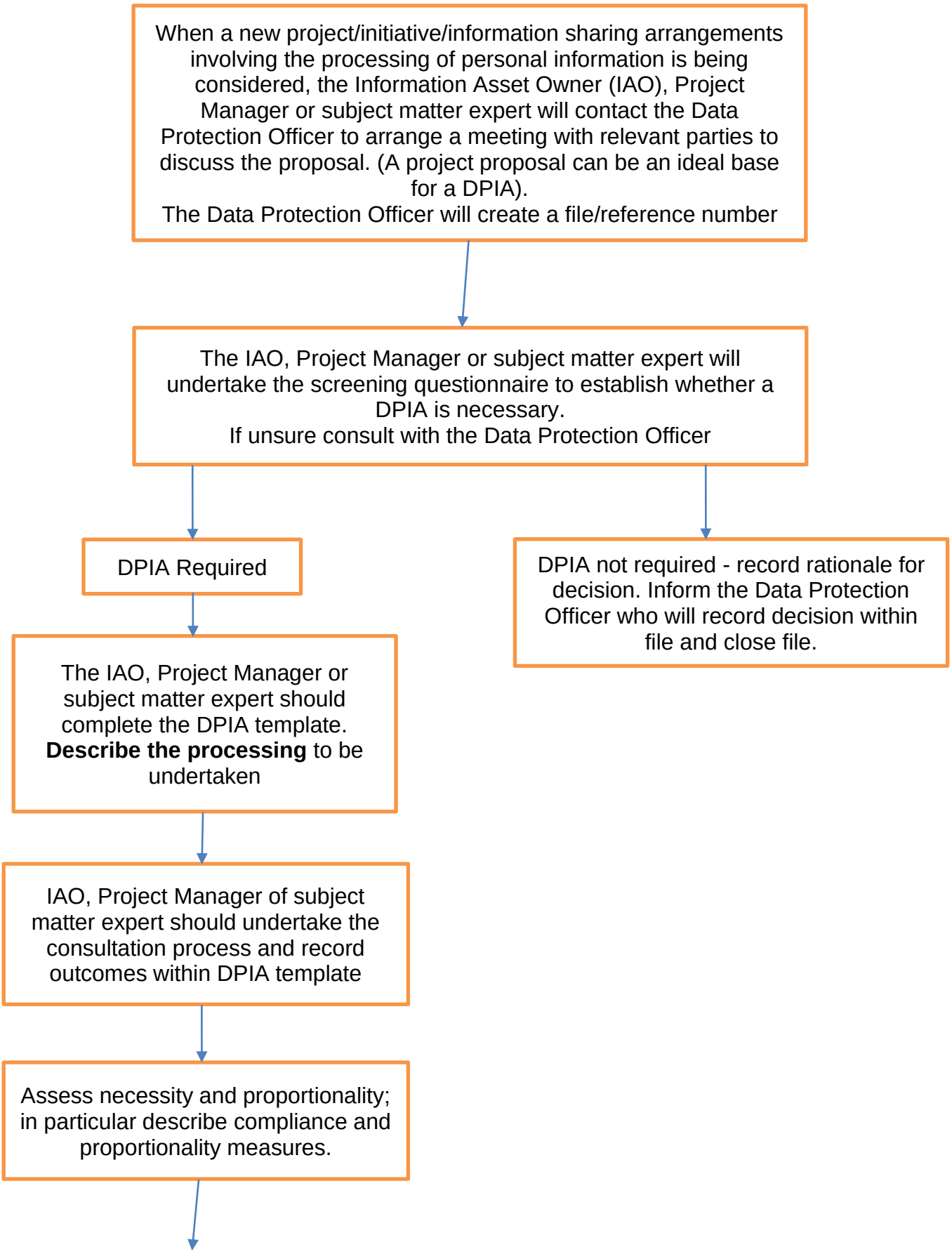
The Corporate Services Department will ensure this document is available on the Force intranet, including any interim updates.

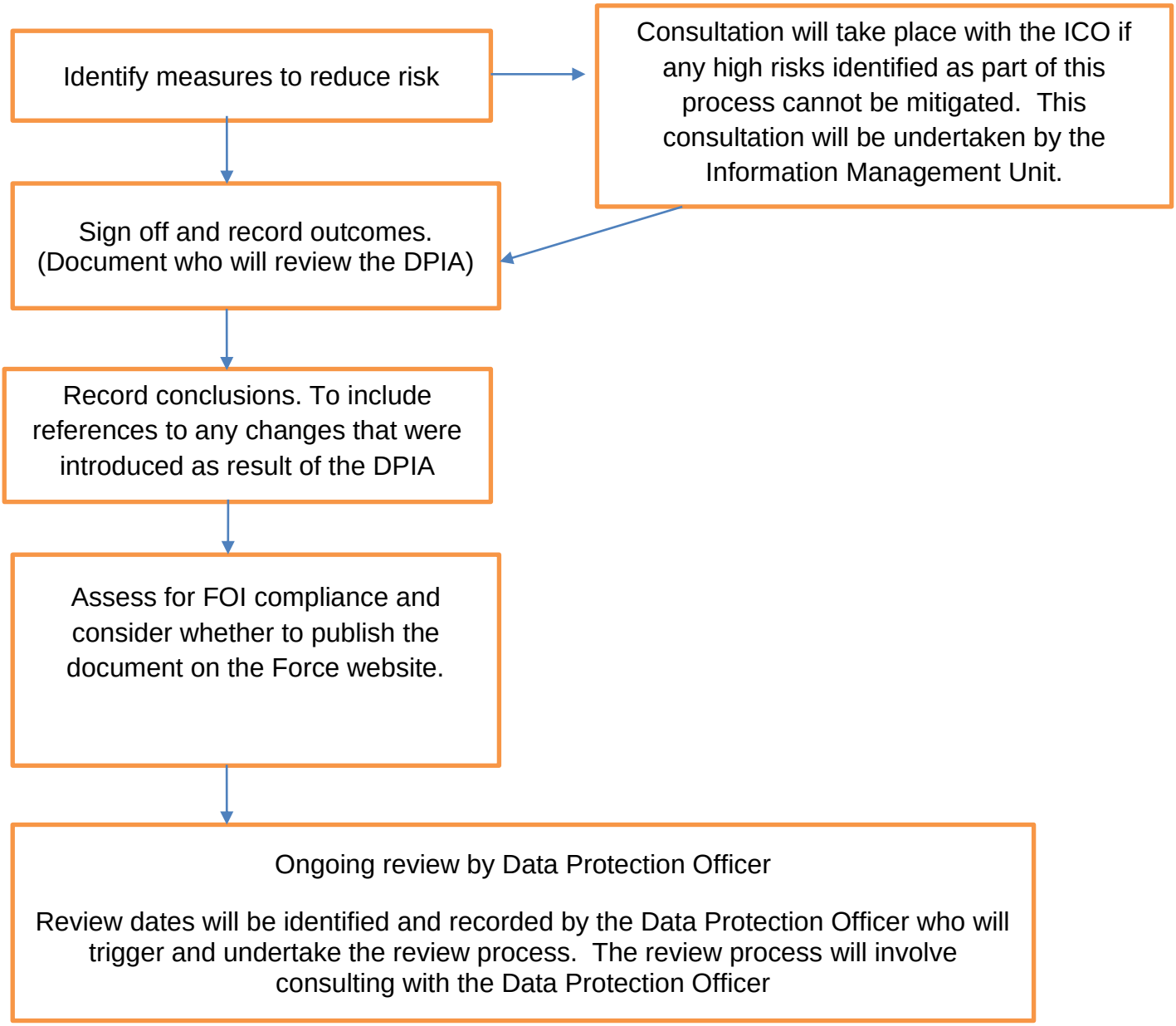
The following identifies all version changes.

Version	Date	Reason for update	Author
0.1	27/07/18	New Policy	[redacted]
0.2	10/10/18	Amended following consultation	[redacted]
1.0	Oct 2018	Policy approved and published	[redacted]
1.1	25/01/21	Policy reviewed	[redacted]
1.2	11/08/21	Amends to tighten up criteria for DPIAs, links to process and details responsibilities	[redacted]
1.3	14/01/22	Updates to two hyperlinks in Section 5	[redacted]

Appendix 1

Information Management Unit
Data Protection Impact Assessment Process




Identify measures to reduce risk
Consultation will take place with the ICO if any high risks identified as part of this process cannot be mitigated. This consultation will be undertaken by the Information Management Unit.
Sign off and record outcomes. (Document who will review the DPIA)
Record conclusions. To include references to any changes that were introduced as result of the DPIA
Assess for FOI compliance and consider whether to publish the document on the Force website.
Ongoing review by Data Protection Officer
Review dates will be identified and recorded by the Data Protection Officer who will trigger and undertake the review process. The review process will involve consulting with the Data Protection Officer