Corporate Procedures

Data Protection Impact Assessment

Date Created:	January 2018	
Version:	V1.0	
Location:	Governance	
Author (s) of Document:	Helen Cannings, Information Governance Team Steven Inglis, Legal Services	
Approval Authority	Senior Information Risk Owner, in consultation with the Convenor & Vice Convenor of Finance, Policy & Resources Committee	
Scheduled Review:	January 2019	
Changes:	January 2018	Previous Privacy Impact Assessment templates have been superseded by this Data Protection Impact Assessment procedure and templates, which have been drafted to comply with the General Data Protection Regulation

ABERDEEN CITY COUNCIL / Shaping Aberdeen

Information Matters

take your time and get it right

Corporate Data Protection Procedures

Data Protection Impact Assessment

1. **About this procedure**
2. **Why is assessing Data Protection Impact important?**
3. **What is a Data Protection Impact Assessment?**
4. **What is a Data Protection Impact Assessment?**
5. **What sorts of projects or proposals will benefit from a Data Protection Impact Assessment?**
6. **What can a Data Protection Impact Assessment achieve?**
7. **Do I need to assess Data Protection Impact?**
8. **Initial Data Protection Impact Assessment Screening**
9. **Brief Data Protection Impact Assessment**
10. **Full Data Protection Impact Assessment**

APPENDIX 1: Initial Data Protection Impact Assessment Screening Questions

APPENDIX 2: Brief Data Protection Impact Assessment Template

APPENDIX 3: Full Data Protection Impact Assessment Template

1. About this procedure

This Procedure and associated templates set out the Council's process for assessing Data Protection Impact.

This procedure supports the Council's Corporate Information Policy, and is a key part of making sure that the way we govern and use our information fulfils our policy objectives to:

- respect privacy and foster trust
- demonstrate accountability through openness

2. Why is assessing Data Protection Impact important?

Our customers and staff care how their information is handled. They're more likely to engage with us if we can demonstrate openly and transparently that we think carefully when we make decisions where personal information or privacy is involved.

By managing privacy successfully, and showing that we take care of personal information, the Council will be better able to meet our customers and our staff's expectations. By contrast, our customers and staff are likely to quickly lose trust in us if we don't treat their information properly or make decisions where we are perceived to intrude on their privacy.

So, while protecting privacy is something that the Council is legally required to do, there are other good reasons for taking care with personal information. How can the Council know whether a new proposal or a new way of handling information will be likely to comply with data protection law, or otherwise affect its customers' or staff's privacy, for better or for worse?

The answer is to do a Data Protection Impact Assessment (DPIA). This way the Council will be able consider the potential data protection and privacy impacts of our decisions and to demonstrate that we have done so. This is a key part of making sure that the way we govern and use our information fulfils our policy objectives to:

- respect privacy and foster trust
- demonstrate accountability through openness

3. What is a Data Protection Impact Assessment?

A DPIA is a practical tool which allows us to:

- identify whether a proposal (e.g. project or initiative) is likely to impact on the privacy of people affected by it, whether positively or negatively;
- check whether a proposal is likely to comply with data protection law and other laws which relate to privacy; and
- make decisions about whether and how to adjust the proposal to manage any privacy and compliance risks identified; and
- it acts as a reference point for future action as the project or the business changes.

4. What sorts of projects or proposals will benefit from a Data Protection Impact Assessment?

- Outsourcing a business or IT service where personal information is going to be held or processed off-site (even off-shore) or may be accessible to the host provider (e.g. storing or processing personal information in the 'cloud')
- Developing data analytics to analyse existing customer information so you can better target services or advertising
- A policy change, or new legislation, that requires sharing of personal information between different agencies, or collecting new information from individuals
- Developing a website or mobile app that collects names, contact information, or locations; or that allows the customer to share information with others
- A major change project to introduce a new business process and supporting IT tools (e.g. switching from requiring clients to fill in paper forms to enabling them to access services and information online)
- Installing a new CCTV camera system, or using other technology to oversee an area where individuals might be or to monitor activities

5. What can a Data Protection Impact Assessment achieve?

A DPIA can identify problems and opportunities early, and make it easier and cheaper to address them. It's much simpler to build in good privacy management throughout the process, rather than trying to bolt it on at the end. It will not be possible to identify and eliminate every risk, or identify every opportunity, and a DPIA does not aim to do so. However, it gives you a good chance of identifying the most serious and the most likely problems.

A DPIA should generally not be a "once-and-for-all" exercise. If your project is long-running, has different phases, or changes over time, then it's worth going back to the DPIA to update it, or even doing a fresh version.

Although this procedure focuses on using a DPIA as part of assessing and managing change, you can also use a DPIA to assess how good existing systems are.

6. Do I need to assess Data Protection Impact?

There are certain circumstances where it is **mandatory** for the Council to carry out a DPIA, and where failure to do so could result in enforcement action, which could lead to a penalty of up to €10 Million.

There's also a risk that not carrying out a Data Protection Impact Assessment will mean that we make decisions or take actions which do not comply with data protection law, and which do not appropriately respect the privacy of the people whose data we process. This may also expose us to significant financial penalty/loss, but more importantly, we risk losing the trust of our customers and staff.

All proposals involving personal information need to comply with data protection law. Data protection law is based around the Data Protection Principles and aims to give

individuals more control over the way their information is handled by organisations like the Council.

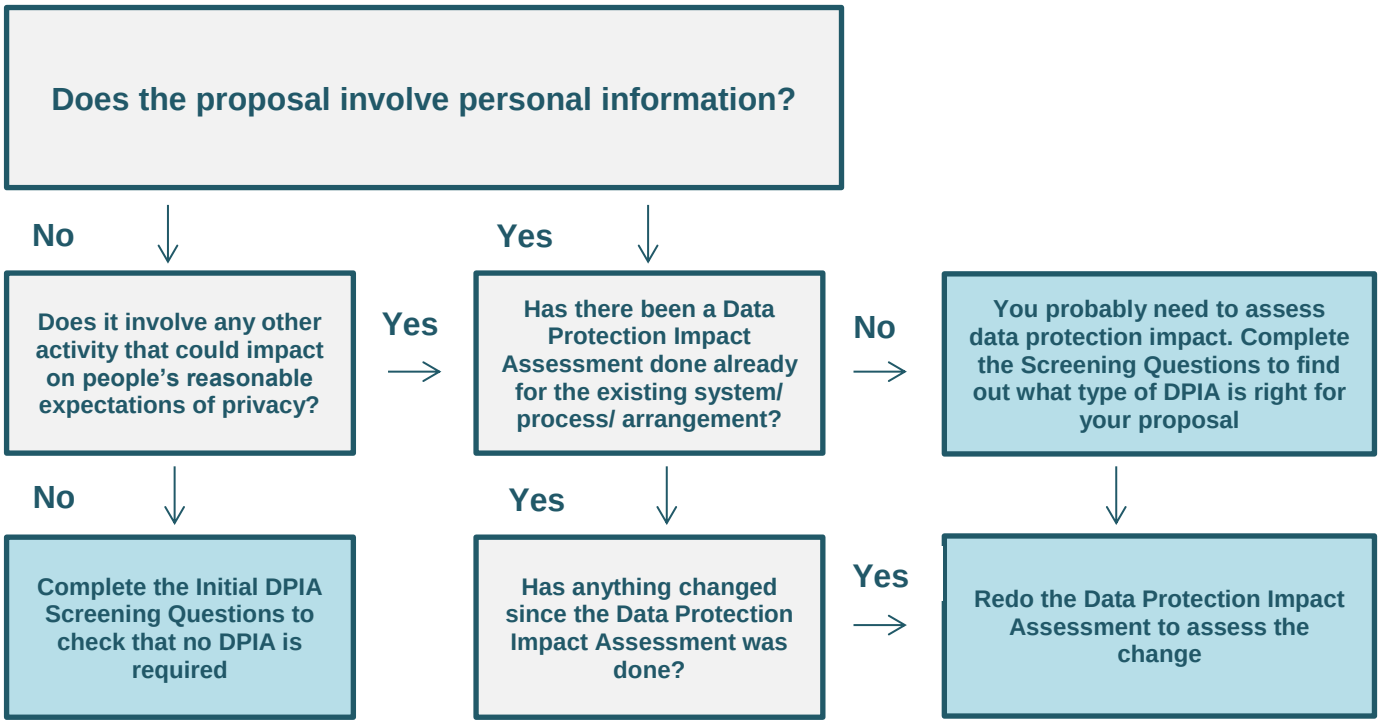
Some proposals or projects are likely to pose higher risks to the privacy of individuals or to the Council's compliance with data protection law. In order to make sure that:

- all our activities comply with data protection law, and
- assessment of data protection impact is proportionate to the risks involved

The Council has adopted a three tier approach to assessing data protection impact:

- Initial DPIA Screening Questions
- A Brief DPIA
- A Full DPIA

The flowchart below sets out how to decide if your project or proposal needs to involve an assessment of data protection impact:



7. Initial Data Protection Impact Assessment Screening

Any proposals which involve personal information or any other activities that could have privacy implications require you to undertake, as a minimum, the Initial DPIA Screening at **Appendix 1** of this Procedure. There are 4 steps to the Initial DPIA Screening process:

STEP 1: Full Data Protection Impact Assessment Criteria

Assess your proposal against the Full Data Protection Impact Assessment Criteria.If your proposal meets any one of the criteria in the Full DPIA Criteria Checklist, then you must undertake a full DPIA, and you should proceed to Step 3. If your proposal does not meet any one of these criteria, proceed to Step 2.

STEP 2: Brief Data Protection Impact Assessment Criteria

Assess your proposal against the Brief Data Protection Impact Assessment Criteria. If your proposal meets any of the criteria in the Brief DPIA Criteria Checklist, then you must undertake a Brief DPIA. Proceed to Step 3.

STEP 3: Record your findings

Use the box provided to record the result of the Initial DPIA Screening process

STEP 4: Sign Off and next steps

Complete the sign off section of the Initial DPIA Screening process.

Where the Initial DPIA Screening Questions indicate that no further assessment of data protection impact is required, the completed screening questions should accompany your proposal through the approval process so decision makers can have assurance that no further DPIA was required.

8. Brief Data Protection Impact Assessment

If the Initial DPIA screening has indicated that you should undertake a Brief DPIA, then you should use the template at **Appendix 2** to allow you to record your findings, conclusions and recommendations.

In most cases, a Brief Data DPIA will be adequate where there are no significant risks to privacy or data protection compliance, but the outcome and recommendations made in the Brief DPIA will inform whether a full DPIA is required.

There are 8 steps to a Brief DPIA:

STEP 1: Provide a Brief description of the proposal or project

In this section give a brief overview of your proposal or project, including:

- Describe your existing systems and the main changes that are proposed
- Describe the purpose of the change, including any projected benefits to your organisation or to the individuals affected
- Identify the main stakeholders or entities involved, and their role in the project.

You may find it helpful to link to other relevant documents related to the project, for example, a project proposal.

STEP 2: Describe the Personal information that the project will involve

Use the table provided in the template to record all the types of different types of personal data which are involved in the proposal or project.

STEP 3: Check how your proposal measures up against the data protection requirements

This step is about assessing your proposal against the requirements of data protection law, and considering where your proposal may raise compliance risks. The checklist will help you to evidence that your proposal has considered and will be compliant with these requirements. For each requirement, consider:

- Is the requirement relevant to your project?
- If yes, identify what personal information is relevant to that requirement?
- Is the change consistent with that data protection requirement? Or will it enhance the Council's compliance?
- Does the change create more risks of harm to the individual? If so, how might it adversely affect the individual? Or does the change eliminate or reduce risk in the existing system

STEP 4: Initial risk assessment

If you identified any risks in relation to compliance with any of the principles or requirements at STEP 3, use the Initial Risk Assessment table provided in the template to give a rating, either:

- Low (L)
- Medium (M)
- High (H)

For each of the aspects of the project set out in the first column: For risks that you've identified as Medium or High, indicate (in the right-hand column) how the project plans to lessen the risk (if this is known).

STEP 5: Summary of data protection impact

Use the table provided in the template to give a summary of the data protection impact rating.

STEP 6: Reasons for the data protection impact rating

Briefly explain here the reasons for the impact rating.

STEP 7: Recommendation

Use the Brief DPIA template to record your decision.

STEP 8: Sign Off and next steps

Whatever the outcome of the Brief Data Protection Impact Assessment, the recommendations **must** be signed off by:

The relevant Information Asset Owner (Third Tier Manager)
This is because the Council's Information Asset Owners are responsible and accountable for the way that their information assets are governed and used, and must be involved in decisions which involve the processing of information assets for which they are accountable.

The Council's Data Protection Officer
The Council is required by law to involve our Data Protection Officer in **all decisions which involve the processing of personal data**, so this is an important element of demonstrating compliance in this area.

- **If a Full Data Protection Impact Assessment is <u>not</u> required**

The appropriately signed off Brief DPIA document **must** accompany your proposal through the relevant approval process, so decision makers can understand why a full DPIA is not needed in this case, and to have appropriate oversight and assurance around the proposal's impact on the Council's compliance with Data Protection law, and the privacy of our customers and staff more broadly.

Keeping a store of key information about data protection and privacy will make each new DPIA process you undertake easier. If questions arise later about whether and how you considered data protection and privacy as part of your process, you can also use this record to demonstrate that you took data protection and privacy seriously and to show the basis of the decision.

- **If a Full Data Protection Impact Assessment <u>is</u> required**

The information you record in the Brief DPIA process will form the basis for going on to do the full DPIA. The Brief DPIA provides a good platform to get further details and do more in-depth analysis.

9. Full Data Protection Impact Assessment

The Council's **Data Protection Officer** must be involved throughout the process of undertaking a full Data Protection Impact Assessment to provide advice and support, on the process. There are 11 steps to a Full DPIA as follows:

STEP 1: Gather the information you need

The information you put together when you were deciding whether to do the Data Protection Impact Assessment will be a good start for doing the full impact assessment. Now is the time to gather together all the details about what personal information the proposal involves and what is going to happen to it.

In this section of the Full DPIA template you should record here any documents which you have relied or referenced in undertaking the DPIA.

STEP 2: Describe the proposal or project

A Data Protection Impact Assessment is a tool to help you achieve the aims of your project or proposal more generally while also protecting personal information and privacy. There is often more than one way of designing a project to accomplish what is intended: a Data Protection Impact Assessment will help to identify the least intrusive way of achieving that aim.

A major key to success is having a clear understanding of what the change is aiming to achieve, and how it will support the Council's work.

In this section you should describe the proposal or project and what it intends to achieve by addressing the following key points:

- Describe the project as a whole
- Where does the Data Protection Impact Assessment sit within the project?
- What is the purpose of doing a Data Protection Impact Assessment?
- What is the organisation trying to achieve with this project?
- Is the project a one-off initiative or part of ongoing business development?
- How does the Council currently manage data protection and privacy in relation to this process or activity? Show where the change that the project involves will fit with the current systems.

It's likely that much of this information required for this section can be collated from existing project documentation.

STEP 3: Who will be involved in the Data Protection Impact Assessment process?

Many of the people with information you need for the Data Protection Impact Assessment are likely to already be involved in the project. However, there may be some external stakeholders you also need to talk to. Make sure you're aware of who has the information you need, and when they're going to be available.

The Council **Data Protection Officer** must be involved in the Data Protection Impact Assessment process; their advice and view must be documented as part of the Data Protection Impact Assessment.

Depending on the nature of your proposal, in addition, the following groups may need to be involved in the Data Protection Impact Assessment process:

Data Processors (Third Parties)

If your proposal involves processing of personal data carried out wholly or in part by a third party (a data processor) then the Data Processor should be involved in the Data Protection Impact Assessment Process.

Individuals involved (Data Subjects or their representatives)

The views of individuals involved could be sought through a variety of means, depending on the proposal and the individuals affected – e.g. for a proposal impacting on staff, it may be appropriate to include trade unions or staff groups in the process.

For a proposal which will impact on external customers it may be appropriate to use customer forums, focus groups or surveys to seek their views on the proposal.

If the Council's final decision on the proposal differs from the views of the data subjects, its reasons for going ahead or not should be documented.

The Data Protection Impact Assessment should also document its justification for not seeking the views of data subjects, if it is decided that this is not appropriate.

Council ICT Security staff

ICT staff will be able to provide information on the systems being used, how the personal information will flow through the system (including how it will be stored and processed), and whether there are any security implications arising which need to be addressed as part of the proposal.

Council Risk and Assurance staff

Council staff who specialise in risk and assurance will be able to provide help and support in identifying risk, controls and mitigations.

Other specialist staff groups

Specialist staff groups who are affected by any proposals for handling personal information, such as customer service or human resources staff, are likely to have invaluable information on how any proposed mitigations are likely to work in practice.

STEP 4: Outline the Scope of the Full DPIA

This step is where you should outline the scope of the DPIA. Describe what the Data Protection Impact Assessment covers and what it doesn't cover. For example:

- What parts of the organisation, project, systems, or IT infrastructure are included?
- What are the information-management processes that the Data Protection Impact Assessment will consider (such as use, storage, access, retention and disposal)?
- What are the limitations of the Data Protection Impact Assessment? For example, it might not cover the use of personal information by a third party if there is no direct control or agreement in place to manage the relationship.

STEP 5: Map the Personal information flows

Identify the personal information involved and document the flow of this information through your systems and processes. An information flow diagram is often the clearest way to do this.

- Describe both the **current** and **future** information flows so that the differences are visible at a glance. Show, for example:
- what personal information is collected and used, and how it flows through the system
- how the project will change the information flow
- all changes to personal information involved in the project – for instance: is new personal information being collected? Where is it coming from?
- Will information that the organisation already holds be used for a new purpose? Why and how?
- What is the nature of the information collected and the source?
- What measures are in place to ensure the information is accurate and up to date?
- Will the organisation tell the individuals what's happening to their information? How will it tell them?
- How is the information managed, handled or protected?

- Who will have access to the information (whether inside or outside the organisation)?
- How long will the information be retained and how will it be disposed of?

This is a critical part of the Data Protection Impact Assessment process. A good way to do this exercise can be to hold a workshop with all of the relevant stakeholders. Your information flows should directly map back to the purpose of your proposal or project and what it hopes to achieve.

STEP 6: Describe the wider organisational context

It's important to consider data protection and privacy implications in the context of the project as a whole, and in light of how the Council operates: particularly the existing approach to handling personal information.

For example, you'll need to know whether any risk mitigation or other change that you recommend for the project is likely to be workable in the context of the Council as a whole. Considering the wider organisational context will also help you be aware of the likely downstream effect of the project on the Council as a whole and enable you to predict and address potential privacy risks.

For example, if your project involves one Council Directorate or business area collecting a new piece of personal information for a particular purpose, how long will it be before another Directorate decides they could use it too? Anticipating this kind of potential "scope creep" is an important part of any Data Protection Impact Assessment.

STEP 7: Check how your proposal measures up against the data protection requirements

This step is about assessing your proposal against the requirements of data protection law, and considering where your proposal may raise compliance risks. The checklist will help you to evidence that your proposal has considered and will be compliant with these requirements. For each requirement, consider:

- Is the requirement relevant to your project?
- If yes, identify what personal information is relevant to that requirement?
- Is the change consistent with that data protection requirement? Or will it enhance the Council's compliance?
- Does the change create more risks of harm to the individual? If so, how might it adversely affect the individual? Or does the change eliminate or reduce risk in the existing system

If you have already undertaken a Brief Data Protection Impact Assessment, you can use the information collated to help you fill in this section.

STEP 8: Data Protection or Privacy Risk Assessment

A privacy risk is the risk that a proposal will fail to meet individuals' reasonable expectations of privacy, for example, because it will mean the Council does not comply with Data Protection law, or because it unreasonably intrudes into an individual's personal space and personal affairs, or runs contrary to what the Council's relationship with our customers or staff would dictate should happen.

Calculating risk is not simply about assessing whether the project will be legally compliant. It's possible to comply with the law and for the behaviour still to affect whether our customers' reasonable privacy expectations are met.

The nature of the Council's relationship with them may suggest that you should give even better protection than the law requires.

The data protection principles and requirements provide a good framework for asking the right questions, both legal and non-legal, about the impact on the people involved.

Risks to an individual will often directly equate to risks to the Council. Data Protection breaches, as well as exposing the Council to significant adverse financial consequences, will have a direct impact on the Council's reputation, and the loss of trust will probably make it harder and more expensive to meet the aims of the proposal or project.

Consider not only the direct risks from the proposal, but also any knock-on effects. If you take too narrow a lens, you may miss an important, wider effect on the individuals you're dealing with.

How to identify a Privacy Risk

Populate the risk table below with the risks you already know about from the previous steps and identify the likely impact on the individuals.

You can then use that as a basis for a more thorough analysis. Make sure you talk to other people involved in the project, or get a view from an external person who may be able to see risks that you have missed.

Other steps, depending on your project, could be:

- a workshop including the key people involved
- a further desk-top review of documentation
- interviews with key people involved

Common examples of mitigations include:

- minimizing the amount of personal information collected
- better and clearer communication with the individuals
- designing the system to provide better security
- providing training and support for staff to help them get it right

Try to ensure that your mitigation solution is practical and sustainable. Reviewing the project once it is operating will help to identify whether the mitigations are actually working as you've planned.

This section describes the privacy risks you've identified through the Data Protection Impact Assessment process and how you propose to mitigate and manage those risks. It can be useful to link this back to the data protection principles to show why these risks and the proposed actions are relevant.

Note: A Data Protection Impact Assessment doesn't set out to identify and eliminate every possible privacy risk: its role is to identify genuine risks that are not unreasonably small or remote.

STEP 9: Recommendations to minimise impact on privacy

In this section you should outline the recommendations to minimise the impact on privacy based on your risk assessment carried out at STEP 9.

STEP 10: Action Plan

This section of the assessment should describe what actions are being taken (whether short or long term) and how they'll be monitored. There may also be links to other processes in the organisation. For example, a proposed action might relate to security controls (such as restricting access to a system). This will then link in with the Council's security processes.

Reporting on the outcome of the mitigation may be necessary. If the DPIA is being performed as part of a project, then the project is likely to require some reporting on its implementation as part of governance arrangements. Once the project is completed, any on-going privacy monitoring should be incorporated into normal business operations.

In the case of a particularly long or complex programme of work, the DPIA may need to be reviewed a number of times to ensure that it continues to be relevant. This section should describe how this will be achieved.

STEP 12: Sign off and next steps

The appropriately signed off full DPIA **must** accompany your proposal through the relevant approval process, so decision makers can understand the data protection and privacy implications of the proposal, and make an informed decision on that basis.

A DPIA should generally not be a "once-and-for-all" exercise. If your project is long-running, has different phases, or changes over time, then it's worth going back to the DPIA to update it, or even doing a fresh version.

APPENDIX 1: Initial DPIA Screening Questions

STEP 1

Full Data Protection Impact Assessment Criteria

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
Privacy Risk Areas			
Evaluation or scoring, profiling and predicting Especially from aspects concerning the data subject's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements			
Automated-decision making Processing that aims at taking decisions on individuals which have a significant effect on them.			
Systematic monitoring Processing used to observe, monitor or control data subjects. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequenting public (or publicly accessible) space(s)			
Sensitive data This includes special categories of personal data (e.g. information about individuals' political opinions, criminal convictions or offences).			
Data processed on a large scale			

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
The following factors should be considered when determining whether the processing is carried out on a large scale: a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; b. the volume of data and/or the range of different data items being processed; c. the duration, or permanence, of the data processing activity; d. the geographical extent of the processing activity			
Datasets that have been matched or combined e.g. originating from two or more data processing operations performed for different purposes and/or by different data controllers.			
Data concerning vulnerable data subjects Because of the increased power imbalance between the data subject and the data controller, the individual may be unable to consent to, or oppose, the processing of his or her data. For example, employees would often meet serious difficulties to oppose the processing performed by their employer, when it is linked to human resources. Similarly, children can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data. This also concerns more vulnerable segments of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.			
Innovative use or applying technological or organisational solutions			

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
For example, certain “Internet of Things” applications, use of facial recognition or biometric technology could have a significant impact on individuals’ daily lives and privacy. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals’ rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the Council to understand and to treat such risks.			
Data transfer across borders outside the European Union Processing outside the EU needs to be considered as in cases where software providers are based or have services in countries outside the EU. You also need to consider here whether the proposal involves enabling Council employees to have access to personal data whilst outside the EU (potentially relevant to Bring Your Own Device etc.)			
When the processing in itself prevents data subjects from exercising a right or using a service or a contract This includes processing performed in a public area that people passing by cannot avoid, or processing that aims at allowing, modifying or refusing data subjects’ access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan			

If your proposal meets any one of these criteria (i.e. you ticked *any* boxes above) **you must undertake a full DPIA**. The process and template for this is included at **Appendix 3**.

If your proposal **does not** meet any of these criteria, you should move on to STEP 2 and assess whether your proposal meets the criteria for a Brief DPIA.

STEP 2

Brief Data Protection Impact Assessment Criteria

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
A new collection of personal information For example, collecting information about individuals' locations			
A new way of collecting personal information For example, collecting information online rather than on paper forms			
A decision to keep personal information for longer than you have previously For example, changing IT backups to be kept for 10 years when you previously only stored them for 7			
A new use or disclosure of personal information that is already held For example, using information collected as part of the housing benefit assessment to verify eligibility for another entitlement			
A change in the way personal information is stored or secured For example, transferring the storage of personal information into the cloud, or the implementation of a policy which effects a change to the way personal information is stored or secured (e.g. Bring Your Own Device)			
Transferring personal information offshore or using a third-party contractor For example outsourcing the payroll function or storing information in the cloud			

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
A change in policy that results in people having less access to information that you hold about them For example, archiving documents after 6 months into a facility from which they can't be easily retrieved			

If your proposal meets any one of these criteria (i.e. you ticked *any* boxes above) **you must undertake a Brief DPIA**. The template for this is included at **Appendix 2**.

STEP 3: Record your findings

Recommendation	Tick which applies
No further Data Protection Impact Assessment is required	
Do a Brief Data Protection Impact Assessment	
Do a full Data Protection Impact Assessment	

STEP 4: Sign-off and Next Steps

Officer	Signature	Comments
Officer undertaking the Data Protection Impact Assessment Screening	*Signature:* *Date:*	
Information Asset Owner (Third Tier Manager)	*Signature:* *Date:*	

Where the recommendation is no assessment of Data Protection Impact Assessment is required, a copy of the completed Initial DPIA screening must accompany **must accompany your proposal through the relevant approval process**.

APPENDIX 2: Brief Data Protection Impact Assessment Template

STEP 1: Provide a Brief description of the proposal or project

a) Describe your existing systems and the main changes that are proposed

b) Describe the purpose of the change, including any projected benefits to your organisation or to the individuals affected

c) Identify the main stakeholders or entities involved, and their role in the project.

You may find it helpful to link to other relevant documents related to the project, for example, a project proposal.

STEP 2: Describe the Personal information that the project will involve

Type of personal Information	Source of Information	Purpose of information for the project

STEP 3: Check how your proposal measures up against the data protection requirements

Data Protection requirements			
Data Protection Requirement	**Description of personal information, how it will be used, how will it be managed**	**Assessment of compliance**	**Compliance Risks Identified**
Principle 1 Personal data shall be processed lawfully, fairly and transparently	*Factors to consider:* *All processing of personal data requires a legal basis in data protection law… is there an appropriate legal basis in data protection law for processing the information?* *Are there any other laws which relate to the use or processing of this information? What are they? Is this proposal compliant with other laws? Is the processing fair?* *Could it seem unexpected or unfair to the individuals involved? How will you tell individuals about what their data is being used for and how it is managed?* *What risks may arise as part of your proposal or project round compliance with this principle?*		

Principle 2 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes	*Does this proposal involve re-using personal information held by the Council for a different purpose? If so, have you identified an appropriate legal basis for the proposed processing of this information?* *Or is there an exemption justifying this use?* *Does this proposal involve processing personal information in a way which is different to what we have told data subjects? Is it fair? Would it be unexpected to individuals involved?* *How will you communicate this new use with individuals affected?* *What risks may arise as part of your proposal or project round compliance with this principle?*		
Principle 3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	*Could the purpose of the proposal or project be achieved without using personal information?* *How will the proposal ensure that only information required to meet the purpose is processed?* *Will the information in scope be enough to achieve the stated purpose?* *What risks may arise as part of your proposal or project round compliance with this principle?*		

Principle 4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	*How will this proposal make sure that any information collected, used, or otherwise processed is accurate? (Reasonable steps will vary depending on the information involved)* *Relevant factors include: what process is there to check that information is correct? Has the information been supplied by the individual directly? Has it been checked with the individual directly?* *How will the proposal ensure that the accuracy of any personal data is maintained over the time it is retained by the Council?* *How damaging will it be to the individual if information is wrong or misleading? (The more damaging it will be, the more extensive should the steps be for checking accuracy)* *If your proposal involves personal information which must be retained by the Council for a long period of time, how will this proposal ensure that the accuracy and integrity of the information is maintained across this period? Retention periods for some types of Council data can often be longer than the lifecycle of the system they are created in. How will your proposal maintain personal data of this type of manage any digital preservation risks?* *What risks may arise as part of your proposal or project round compliance with this principle?*		

Principle 6 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;	*Are there any statutory obligations or business reasons to hold the information for a specific period of time, as set out in the Council's Retention & Disposal Schedule?* *If no such obligations exist, how long do we need to keep the information? This should always be no longer than is necessary, and is linked to the purposes for which we collect it in the first place?* *Remember: we need to tell our customers how long we're keeping information about them when we collect the information, as part of the privacy notice, so you need to make sure that your proposal* *How will retention and disposal (or anonymization) work in practice? Who will do it? How will it be done? When and how frequently? Will it be an automated or a manual process? How will we ensure that personal information is securely destroyed?* *What risks may arise as part of your proposal or project round compliance with this principle?*		

Principle 5 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	*What technical measures will need to be in place to secure the data involved?* *What measures need to be in place to make sure only those required to access the data are able to do so?* *Will the proposal require any policies, procedures or guidance to be updated or new ones put in place?* *Will the proposal mean that staff need training to ensure data is used or secured appropriately?* *Will an ICT security risk assessment be required to identify vulnerabilities? If not, why not? How will any controls and mitigations identified be implemented?* *What risks may arise as part of your proposal or project round compliance with this principle?*		
Principle 7 The Council is responsible for, and able to demonstrate compliance with, the above data protection principles	*The Council is required to be able to proactively demonstrate compliance with all principles above. How will this requirement be factored into the design and implementation of your system/ initiative/ project? What risk may arise around compliance with this principle?*		

Third Parties The Council must be able to evidence robust arrangements with third parties who process data on our behalf, which set out our requirements in relation to compliance with data protection law. Without such arrangements the Council can be held liable for non-compliance of such third parties, which may result in enforcement action and monetary penalties.	*Will this proposal or project involve third parties processing personal data on behalf of the Council?* *Third parties could include software providers, public sector partners, or other service providers where personal information is involved as part of providing the service on our behalf*. *Appropriate contractual arrangements or data sharing agreements will need to be in place which set out how the third parties will comply with the data protection principles. How will this requirement be met in practice? What risks may arise as part of your proposal or project round compliance with this principle?*		

People's Rights Individuals have certain rights under data protection law.	*Individuals have a range of legal rights in relation to their data. Will your proposal support or manage these rights? Are arrangements in place for recognizing and responding to requests for access to individuals' personal data? What risks may arise as part of your proposal or project round compliance with this requirement?*		
Other Privacy Risk Areas	*Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of CCTV, Automatic number plate Recognition (ANPR), body worn cameras, biometrics or facial recognition?*		

STEP 4: Initial risk assessment

Aspect of the Project	Rating (L, M or H)	Describe any medium and high risks and how to mitigate them
Level of information handling L – Minimal personal information will be handled M – A moderate amount of personal information (or information that could become personal information) will be handled H – A significant amount of personal information (or information that could become personal information) will be handled		
Sensitivity of the information (e.g. health, financial, race) L – The information will not be sensitive M – The information may be considered to be sensitive H – The information will be highly sensitive		
Significance of the changes L – Only minor change to existing functions/activities M – Substantial change to existing functions/activities; or a new initiative H – Major overhaul of existing functions/activities; or a new initiative that's significantly different		
Interaction with others L – No interaction with other organisations M – Interaction with one or two other organisations H – Extensive cross-organisation interaction		

Public impact L – Minimal impact on individuals M – Some impact on individuals is likely due to changes to the handling of personal information; or the changes may raise public concern H – High impact on individuals, and concerns over aspects of project; or negative media publicity is likely		

STEP 5: Summary of data protection impact

The privacy impact for this project has been assessed as:	Tick
Low – There is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm is negligible; or the change is minor and something that the individuals concerned would expect; or risks are fully mitigated	
Medium – Some personal information is involved, but any risks can be mitigated satisfactorily	
High – Sensitive personal information, or large volumes of personal data, is involved, and several medium to high risks have been identified	
Reduced risk – The project will lessen existing privacy risks	
Inadequate information – More information and analysis is needed to fully assess the privacy impact of the project.	

STEP 6: Reasons for the data protection impact rating

Briefly summarise the reasons for the ratings that you have given at STEP 5.

STEP 7: Recommendation

Recommendation	Tick which applies
Do a full Data Protection Impact Assessment	
Data Protection compliance and privacy risk can be adequately managed through the Brief Data Protection Impact Assessment	

STEP 8: Sign off

Whatever the outcome of the Brief Data Protection Impact Assessment, the recommendations **must** be signed off by:

- **The relevant Information Asset Owner (Third Tier Manager)**

This is because the Council's Information Asset Owners are responsible and accountable for the way that their information assets are governed and used, and must be involved in decisions which involve the processing of information assets for which they are accountable.

- **The Council's Data Protection Officer**

The Council is required by law to involve our Data Protection Officer in **all decisions which involve the processing of personal data**, so this is an important element of demonstrating compliance in this area.

Officer	Signature	Comments
Officer undertaking the Brief Data Protection Impact Assessment	*Signature:* *Date:*	
Information Asset Owner (Third Tier Manager)	*Signature:* *Date:*	
Data Protection Officer	*Signature:* *Date:*	

The appropriately signed off Brief Data Protection Impact Assessment document **must accompany your proposal through the relevant approval process**, so decision makers can understand why a full Data Protection Impact Assessment is not needed in this case, and to have appropriate oversight and assurance around the proposal's impact on the Council's compliance with Data Protection law, and the privacy of our customers and staff more broadly.

APPENDIX 3: Full Data Protection Impact Assessment Template

STEP 1: Gather the Information you need

Record here any documents which you have relied on in undertaking this DPIA, or have referenced later in this DPIA.

STEP 2: Describe the project or proposal – especially the purpose of changing what happens with personal information

STEP 3: Outline the scope of the Data Protection Impact Assessment

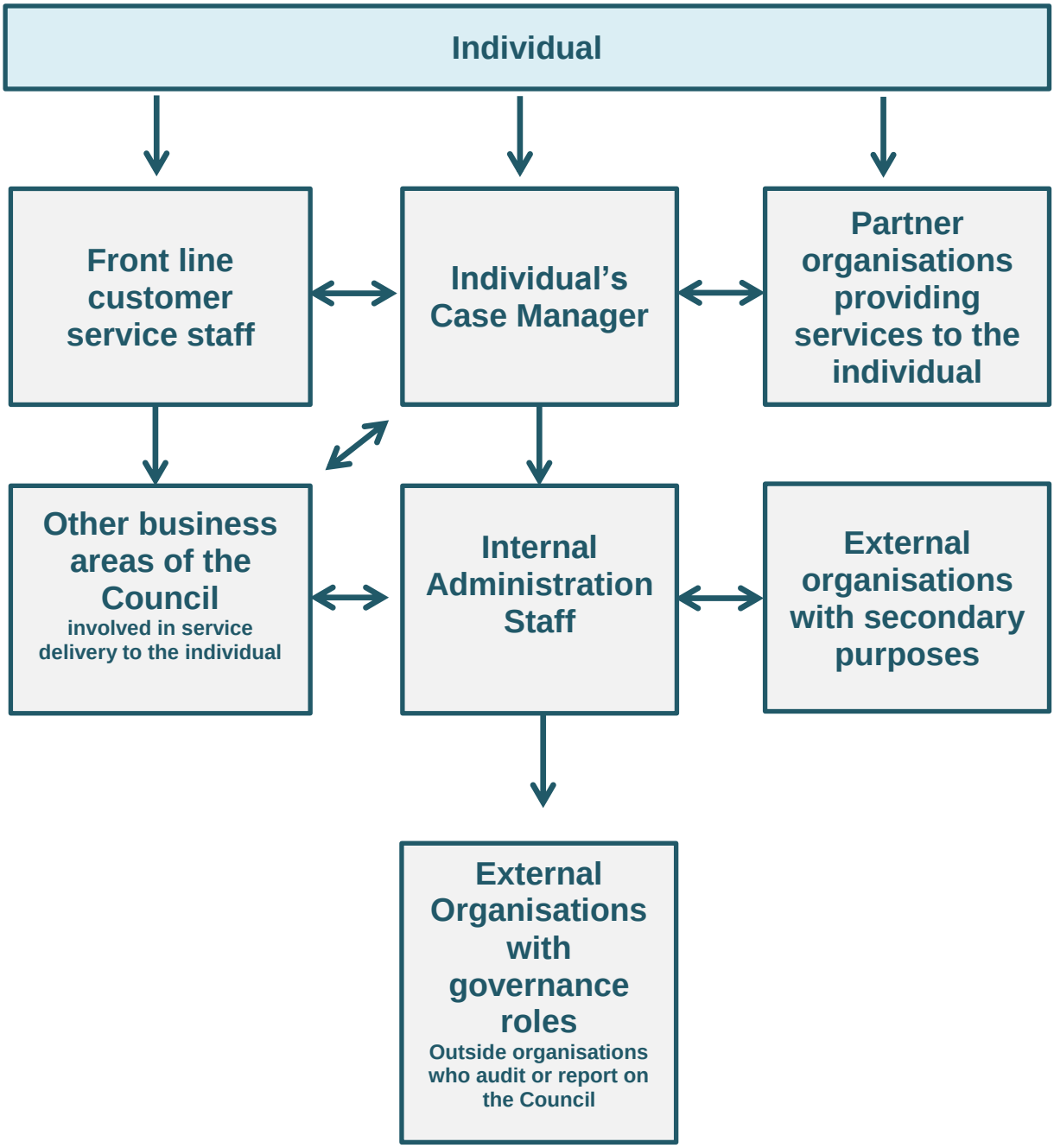
STEP 4: Who will be involved in the Data Protection Impact Assessment process?

Outline here who was consulted and why. Include justification for not consulting individuals affected or their representatives if relevant.

STEP 5: Explain the scope and process

STEP 6: Explain and map the Personal information flows

Example Information Flow Diagram (to be customised)



STEP 7: Describe the organisational context

STEP 7: Check how your proposal measures up against the data protection requirements

If you have already undertaken a Brief Data Protection Impact Assessment, you can use the information collated to help you fill in this section.

Data Protection Requirement	**Description of personal information, how it will be used, how will it be managed**	**Assessment of compliance**	**Compliance Risks Identified**
Principle 1 Personal data shall be processed lawfully, fairly and transparently	*Factors to consider:* *All processing of personal data requires a legal basis in data protection law… is there an appropriate legal basis in data protection law for processing the information?* *Are there any other laws which relate to the use or processing of this information? What are they? Is this proposal compliant with other laws? Is the processing fair?* *Could it seem unexpected or unfair to the individuals involved? How will you tell individuals about what their data is being used for and how it is managed?* *What risks may arise as part of your proposal or project round compliance with this principle?*		

Principle 2 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes	*Does this proposal involve re-using personal information held by the Council for a different purpose? If so, have you identified an appropriate legal basis for the proposed processing of this information?* *Or is there an exemption justifying this use?* *Does this proposal involve processing personal information in a way which is different to what we have told data subjects? Is it fair? Would it be unexpected to individuals involved?* *How will you communicate this new use with individuals affected?* *What risks may arise as part of your proposal or project round compliance with this principle?*		
Principle 3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	*Could the purpose of the proposal or project be achieved without using personal information?* *How will the proposal ensure that only information required to meet the purpose is processed?* *Will the information in scope be enough to achieve the stated purpose?* *What risks may arise as part of your proposal or project round compliance with this principle?*		

Principle 4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	*How will this proposal make sure that any information collected, used, or otherwise processed is accurate? (Reasonable steps will vary depending on the information involved)* *Relevant factors include: what process is there to check that information is correct? Has the information been supplied by the individual directly? Has it been checked with the individual directly?* *How will the proposal ensure that the accuracy of any personal data is maintained over the time it is retained by the Council?* *How damaging will it be to the individual if information is wrong or misleading? (The more damaging it will be, the more extensive should the steps be for checking accuracy)* *If your proposal involves personal information which must be retained by the Council for a long period of time, how will this proposal ensure that the accuracy and integrity of the information is maintained across this period? Retention periods for some types of Council data can often be longer than the lifecycle of the system they are created in. How will your proposal maintain personal data of this type of manage any digital preservation risks?* *What risks may arise as part of your proposal or project round compliance with this principle?*		

Principle 6 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;	*Are there any statutory obligations or business reasons to hold the information for a specific period of time, as set out in the Council's Retention & Disposal Schedule?* *If no such obligations exist, how long do we need to keep the information? This should always be no longer than is necessary, and is linked to the purposes for which we collect it in the first place?* *Remember: we need to tell our customers how long we're keeping information about them when we collect the information, as part of the privacy notice, so you need to make sure that your proposal* *How will retention and disposal (or anonymization) work in practice? Who will do it? How will it be done? When and how frequently? Will it be an automated or a manual process? How will we ensure that personal information is securely destroyed?* *What risks may arise as part of your proposal or project round compliance with this principle?*		

Principle 5 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	*What technical measures will need to be in place to secure the data involved?* *What measures need to be in place to make sure only those required to access the data are able to do so?* *Will the proposal require any policies, procedures or guidance to be updated or new ones put in place?* *Will the proposal mean that staff need training to ensure data is used or secured appropriately?* *Will an ICT security risk assessment be required to identify vulnerabilities? If not, why not? How will any controls and mitigations identified be implemented?* *What risks may arise as part of your proposal or project round compliance with this principle?*		
Principle 7 The Council is responsible for, and able to demonstrate compliance with, the above data protection principles	*The Council is required to be able to proactively demonstrate compliance with all principles above. How will this requirement be factored into the design and implementation of your system/ initiative/ project? What risk may arise around compliance with this principle?*		

Third Parties The Council must be able to evidence robust arrangements with third parties who process data on our behalf, which set out our requirements in relation to compliance with data protection law. Without such arrangements the Council can be held liable for non-compliance of such third parties, which may result in enforcement action and monetary penalties.	*Will this proposal or project involve third parties processing personal data on behalf of the Council?* *Third parties could include software providers, public sector partners, or other service providers where personal information is involved as part of providing the service on our behalf*. *Appropriate contractual arrangements or data sharing agreements will need to be in place which set out how the third parties will comply with the data protection principles. How will this requirement be met in practice? What risks may arise as part of your proposal or project round compliance with this principle?*		

People's Rights Individuals have certain rights under data protection law.	*Individuals have a range of legal rights in relation to their data. Will your proposal support or manage these rights? Are arrangements in place for recognizing and responding to requests for access to individuals' personal data? What risks may arise as part of your proposal or project round compliance with this requirement?*		
Other Privacy Risk Areas	*Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of CCTV, Automatic number plate Recognition (ANPR), body worn cameras, biometrics or facial recognition?*		

STEP 8: Data Protection & Privacy Risk Assessment

Assessment of potential risks and possible mitigations to reduce or manage adverse effects							
Principle 1:							
Ref. no.		Description of the risk(s)	Rationale and consequences for the Council or individual	Existing controls that contribute to manage risks identified	Assessment of residual current risk	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
Principle 2:							
Ref. no.		Description of the risk(s) identified	Rationale and consequences for the Council or individual	Existing controls that contribute to manage risks identified	Assessment of residual current risk	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
Principle 3:							

Ref. no.		Description of the risk(s) identified	Rationale and consequences for the Council or individual	Existing controls that contribute to manage risks identified	Assessment of residual current risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards

Principle 4:

Ref. no.		Description of the risk(s) identified	Rationale and consequences for the Council or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards

Principle 5:

Ref. no.		Description of the risk(s) identified	Rationale and consequences for the Council or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards

Principle 6:							
Ref. no.		Description of the risk(s) identified	Rationale and consequences for the Council or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards

Principle 7:							
Ref. no.		Description of the risk(s) identified	Rationale and consequences for the Council or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards

Individuals' Rights

Ref. no.		Description of the risk(s) identified	Rationale and consequences for the Council or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards

Third Parties

Ref. no.		Description of the risk(s) identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards

Other Privacy Risks

Ref. no.		Description of the risk(s) identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards

STEP 9: Recommendations to minimise impact on privacy

Ref	Recommendation	Agreed Y/N
R-001		

STEP 10: Action Plan

Ref	Agreed action	Who is responsible	Completion Date
A-001			

STEP 11: Sign Off

Officer	Signature	Comments
Officer undertaking the Data Protection Assessment	*Signature:* *Date:*	
Information Asset Owner (Third Tier Manager)	*Signature:* *Date:*	
Data Protection Officer	*Signature:* *Date:*	