Ref. No.	CO/IG/8
Category:	
People	
Place	
Corporate	Yes
In Constitution	

Data Protection Impact Assessment Policy

Policy Details

What is this policy for?	The Data Protection Impact Assessment (DPIA) Policy describes how the Council will conduct Data Protection Impact Assessments as a key requirement under the GDPR.
Who does this policy affect?	All members, employees, students, apprentices, volunteers, contractors and other third parties handling council information
Keywords	Information Governance, Individual Rights, Right to be Informed, Right to Object, SAR, Right to be Forgotten, Automated Decision Making, Data Breach
Author	Gary McCann, Data Protection Officer
Dorset Council policy adopted from	This is a new policy for Dorset Council, which supersedes any previous sovereign councils' policies in relation to data protection impact assessments.
Does this policy relate to any laws?	Data Protection Act 2018; General Data Protection Regulation (GDPR)
Is this policy linked to any other Dorset Council policies?	This policy is part of the Information Governance Framework, which also includes: • Data Protection Policy • Data Breach Policy • Data Protection Policy • Individual Rights Policy • Confidential Waste, Clear Desk and Screen Policy • Data Quality Policy • Protective Marking Policy • Records Management Policy • Records Retention Policy • Information Security Management Policy and related standards and protocols
Equality Impact Assessment (EqIA)	An EqIA screening tool was completed and submitted on 11th March 2019. The tool identified that there was no need to complete an EqIA.
Other Impact Assessments	N/A

Status and Approvals

Status	Live	Version	1
Last review date	This is a new policy for Dorset Council	Next review date	1 April 2020
Approved by (Director)	Dorset Council Corporate Director: Legal & Democratic	Date approved	26 February 2019
Member/ Partnership Board Approval		Date approved	

Contents

Introduction

The General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 regulate how personal information relating to *natural persons* is managed.

One of the requirements of the legislation is that and processing of personal data "likely to result in a high risk to the rights and freedoms of natural persons" should be preceded by the completion of a Data Protection Impact Assessment (DPIA) (Article 35). This is in accord with another GDPR requirement, "Data protection by design and default" (Article 25),

NEW projects that involve personal confidential data or intrusive technologies give rise to privacy issues and concerns. Privacy embraces the principles of "confidentiality" from legislation like the GDPR and The Data Protection Act 2018 to the common law principle of a duty of confidentiality. An overarching principle of this policy advocates that respect for privacy and dignity should be considered at the outset of any project which risks privacy or confidentiality. To enable the council to address any privacy concerns and risks, a Data Protection Impact Assessment (DPIA), **must** be used

Data Subjects have rights under the GDPR. Those rights include the right;

- to be informed that processing of personal data is being undertaken of access to one's personal data to rectification of personal data
- to erasure ('the right to be forgotten')
- to restriction of processing.
- to be notified of rectified, erased or restricted processing.
- to data portability
- to object to data processing
- to not be subjected to automated decision making

Further, we are required to take appropriate technical and organisational security measures to safeguard personal information in all office and public spaces, on Council owned equipment, including mobile devices, and staff owned personal mobile devices (e.g. laptops, ipads, iphones) which are used to share and process personal and sensitive information. We must also ensure that personal information is not transferred abroad without suitable safeguards. A DPIA is expected to reference all of these rights.

'Special Categories' of Personal Data

The GDPR requires that controlling or processing special categories of personal data without a lawful basis, or explicit consent for one or more specified purposes is prohibited. Those special categories are:

a) Racial or ethnic origin
b) Political opinions
c) Religious or philosophical beliefs
d) Trade union membership
e) Genetic data & biometric data for the purpose of uniquely identifying an individual
f) Health
g) Sex life or sexual orientation
additionally
h) Criminal convictions and offences require control of official authority.

A DPIA is expected to consider these 'special categories'.

Purpose

This policy is designed to be read in association with the DPIA Process & Procedure and the DPIA Guidance Notes.

A Data Protection Impact Assessment aims to ensure systems and processes within the council are fit for purpose and include privacy by design. There **must** be a comprehensive consideration of potential impacts on confidentiality, information quality and security at the design phase of any new process, procurement of a new information asset of new and novel ways of using existing data.

In following this process and ensuring that Data Protection Officer is notified and involved from the initial conception of a project, we can provide assurance the council's information is being handled in a secure and responsible way and complies with legislation.

Important: Not all processing activities will need a DPIA. Please refer to the Guidance Notes

Statement of Policy

Dorset Council processes relevant personal information in the delivery of its services. This includes local residents, current, past and prospective employees, suppliers, clients, customers and others with whom it communicates.

The Council fully endorses and adheres to the Article 25 principle of "Data Protection by design and default", as set out in the GDPR.

Privacy by design

Taking a privacy by design 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, Increasing the likelihood that the initiative is more successful because privacy risks are identified early when addressing them will often be simpler and less costly.
- Increased awareness of privacy and data protection across an organisation. Taking actions which are less likely to be privacy intrusive and have a negative impact on individuals
- Fulfilling the council's legislative, statutory and contractual obligations, particularly those under data protection legislation in relation to data processing activities
- Contributing towards effective risk management and increased privacy and data protection awareness across the institution
- Giving individuals confidence that the council is taking steps to safeguard their privacy, and a better understanding of the ways in which their personal data are being used.

Any processing activities, especially those using new and emerging technologies, or existing technologies in new ways, to process personal data likely to pose a high risk to the right and freedoms of individuals will be subject to the need to consider a DPIA.

Failure to adhere to this policy may result in a financial loss and/or reputational damage to the Council and staff may be subject to disciplinary action for non-compliance with the policy.

Scope

The scope of this document is to outline the council's approach and methodology for DPIA's, current systems that have not had a DPIA before but require new or upgraded services and especially **NEW** systems. (see S5 Application)

It covers all information assets that are paper or electronic within the council.

This DPIA policy is applicable to any member of staff employed by the council, members, private contractors, volunteers and temporary staff who are responsible for project managing a new "project" or "plan" to modify any existing system (information asset).

Application – When do I need to do a DPIA?

You must do a DPIA before you begin any type of processing which is "likely to result in a high risk". Although you have not yet assessed the actual level of risk you need to screen for factors that point to the potential for a widespread or serious impact on individuals. Please see the guidelines for screening questions.

In particular, the GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires you to do a DPIA if you plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

This list is not exhaustive. Other factors will also present a high risk

Retention & Review of DPIAS

A DPIA is the property of the Information Asset Owner. It is the responsibility of the Information Asset Owner to ensure that the DPIA is kept under review during the lifetime of the project.
Each project is to be assessed on its merits. Any review period should form a part of the DPIA
The Retention Period for DPIA's is the lifetime of the project plus 6 years.

Equality Impact Assessment

All relevant persons are required to comply with this document and must demonstrate sensitivity and competence in relation to the nine protected characteristics as defined by the Equality Act 2010. If you believe any other groups are disadvantaged by anything contained in this document please contact the Equality and Diversity Officer who will then actively respond to the enquiry.

Cross reference to other procedural documents

DPIA Guidance is accessible to staff on Sharepoint
DPIA Process & Procedure is accessible to staff on Sharepoint
DPIA template is accessible to staff on Sharepoint
Data Protection Policy
Freedom of Information Policy
Information Security Policy
Risk Management Policy and Procedures
All current policies and procedures are accessible in the policy section of the public website
DPIA Guidance is accessible to staff on Sharepoint.

Associated legislation

The GDPR Article 35
European Convention on Human Rights Article 8
The Data Protection Act 2018
Common Law Duty of Confidentiality

Glossary and definitions

Accreditation of Information Assets – The screening questions and full scale DPIA will form part of the accreditation documentation for an Information Asset
Information Asset – An Information Asset is any data, processed by us. It is held in an electronic or hard copy/manual format. Therefore, we are the data controller.
GDPR – The General Data Protection Regulation
Data Privacy Impact Assessment – (DPIA's) A risk technique advocated by the ICO to enable organisations to address privacy concerns and ensure appropriate safeguards are addressed and built in as projects or plans to develop existing information assets.
Dorset Council is the data controller under the GDPR
A **Data Subject** is an individual who is the subject of personal data
A **Data Controller** is a person or an organisation who determines the purposes and the manner in which any personal data is processed.
A **Data Processor** is any person who processes the data on behalf of the data controller. This includes the Council's Services Units.
Data Processing (in relation to information or data) is the collection, recording and/or holding the information and carrying out any actions using it.
Projects / plans to develop – DPIA's are required when new projects occur (for example introduction of a new electronic human resources or payroll) or where plans are proposed to develop an existing information asset. These can be both paper and electronic
Senior Information Risk Owner (SIRO) Is responsible for identifying all risks to the information and making sure that appropriate procedures are in place so that those risks can be managed[1].
Special Category Data – under the GDPR and Data Protection Act 2018 is data including racial or ethnic origin, political opinions, religious or philosophical beliefs, Trades Union membership, genetic or biometric data for the purpose of uniquely identifying a natural person, health, sex life or sexual orientation. The processing or data relating to criminal convictions also requires special category treatment.

Data Protection Impact Assessment (DPIA) Procedure

Version Control			
Status	Active	Version	1
Effective date	11/12/2018	Authorised by	Gary McCann
Revision due	11/11/2019	Revised by	

Contents

1. Introduction

This procedure is designed to be used in conjunction with Data Protection Impact Assessment (DPIA) Guidance and DPIA policy.

In following this procedure and ensuring that Data Protection Officer (DPO) are notified and involved from the initial conception of the project we can provide assurance the Council's information is being handled in a secure and responsible way and complies with legislation.

Note: The DPIA is only applicable where the proposed new project/system/process or proposed change to a system/process is to use personal confidential or special category (sensitive) data, or significantly change the way in which personal data is handled

Data Subjects have rights under the GDPR.
Those rights include the right to;

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

We are required to take appropriate technical and organisational security measures to safeguard personal information in all office and public spaces, on Council owned equipment, including mobile devices, and staff owned personal mobile devices (e.g. laptops, ipads, iphones) which are used to share and process personal and sensitive information.

Ensure that personal information is not transferred abroad without suitable safeguards

Special Categories' of Personal Data

The GDPR requires that controlling or processing special categories of personal data without a lawful basis, or explicit consent for one or more specified purposes is prohibited. Those special categories are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data & biometric data for the purpose of uniquely identifying an individual
- Health
- Sex life or sexual orientation

additionally

- Criminal convictions and offences require control of official authority.

We must consider a DPIA for any processing of personal data 'likely to result in a high risk'' to the rights and freedoms of individuals. There is no definition of 'high risk' but we need to consider the likelihood and severity of any potential breach to those rights and freedoms.

2. What is a data protection impact assessment? (DPIA)

A DPIA a tool which can help the council identify the most effective way to comply with our data protection obligations and meet Data Subjects rights and expectations of privacy.

The ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach.

The council must comply with the GDPR, the Data Protection Act 2018 and other UK privacy laws when we process such information. The council has drafted this policy following the ICO DPIA good practice guidance and screening questions outlined in

An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and potential damage to reputation, which might otherwise occur.

Consultation with stakeholders may give them assurance that we are processing data competently and with their best interests at heart

3. What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller (see Article 6 GDPR).
- An assessment of the necessity & proportionality of processing in relation to its purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that we comply.
- A DPIA can address more than one processing activity

The relevant provisions in the GDPR – see Articles 35, 36 and 83 and Recitals 84, 89 and 96

4. Do we need to do a DPIA?

We should carry out a DPIA if we plan any new data processing activity likely to result in a high risk to peoples' personal data

The **GDPR** says we **Must** do a DPIA if we plan to:

- use systematic and extensive profiling with significant effects;
- process special-category or criminal-offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale

The ICO says we **Must** do DPIA

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach

We may **not** have to carry out a DPIA if:

- We are processing on the basis of **legal obligation** or **public task**. However, this exception only applies if:
  - we have a clear statutory basis for the processing; or,
  - the legal provision or a statutory code specifically provides for and regulates the processing operation in question; or,
  - we are not subject to other obligations to complete DPIAs, such as mandatory minimum measures required by Cabinet Office for consideration of information governance risks or requirements derived from specific legislation, such as Digital Economy Act 2017; or
  - a data protection risk assessment was carried out as part of the impact assessment when the legislation was adopted. (In the absence of any clear statement on whether such an assessment was conducted we recommend that the council err on the side of caution and conduct a DPIA to ensure we consider how best to mitigate any high risk.)
- We have already done a **substantially similar** DPIA. We need to be confident that we can demonstrate that the nature, scope, context and purposes of the processing are all similar.
- The ICO issues a list of processing operations which do not require a DPIA. The ICO has the power to establish this type of list, but has not done so yet.

5. Who should be involved?

If the screening questions indicate that an assessment is required, the DPIA Team Lead will assess the processing operations that will be involved in the DPIA (using the positively answered screening questions) and decide if any further team members are required. The people who are involved have the authority to support the project

The list below is the very minimum of persons who should be involved in a DPIA. In most cases far more will be.

- A Lead Officer
  This is the person who will carry out the DPIA and should have sufficient responsibility and authority to be able to carry through the DPIA requirements. This person will also be the first contact with the 'Risk and Resilience' team etc
- Information Asset Owner (IAO)
  The person who is currently or will be responsible for the Information Asset. This may be the same person as the Lead Officer
- Data Protection Officer
  Must be involved in all DPIAs. The DPO will offer advice and guidance in line with current best practice and legislation
- ICT data security
  Especially if the asset is an IT one

DPIA guidance is provided for staff members by the Data Protection Officer, as part of the Information Asset Owner training.

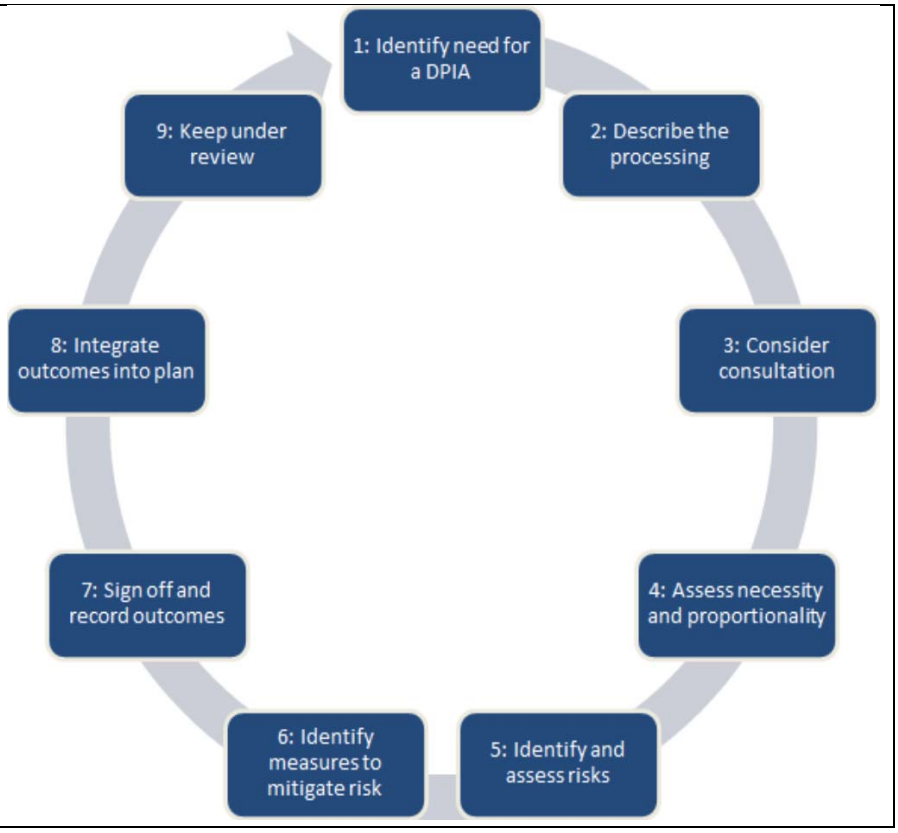
The Data Protection Officer is also responsible for ensuring support and guidance is given when staff members are required to fill out the DPIA.

6. DPIA Stages

A DPIA is an iterative process. It should be constantly reviewed. A DPIA is designed to be flexible and scalable, with time and resources allocated to fit the approach to the risks

A DPIA should be done in stages, to ensure that all aspects are reviewed and documented.

Identify the need for a DPIA
Describe the processing
Consider consultation
Assess the necessity for proportionality
Identify and assess risks
Identify measures to mitigate the risks
Sign off and record outcomes
Integrate outcomes into the project plan
Keep our DPIA under review



The Lead Officer for the DPIA should work closely with the IAO. Between them, they are responsible for ensuring the DPIA is completed and that the DPIA is carried out with support and guidance from other individuals, as relevant, i.e. The Data Protection Officer, ICT etc.

The following process must be followed:

6.1 Identify the need for a DPIA (Screening questions)

Not all processing activities will require a DPIA to be completed, For example, there are exceptions to processing where it is on the basis of a legal or public task and certain conditions are met; see "Do we need to do a DPIA"

If we already know we need a DPIA there is **no need to use the screening questions – Go to the next step "Describe the processing"**

We should always consult the Data Protection Officer if we are unsure.

We consider carrying out a DPIA in any major project involving the use of personal data.

We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

If we decide not to carry out a DPIA, we should document our reasons.

Appendix 1 contains some screening questions that may help us to decide. The questions are not exhaustive.

6.2 Describe the processing

How do we use the data. We need to look at the;

- **Nature** of the processing - what we plan to do with the personal data; and
- The **scope** of the processing - what the processing covers; and
- The **context** of the processing – internal and external factors affecting the data; The wider picture. Things that might affect expectations or outcomes
- The **purpose** of the processing – the reason why we would want to process the data.

6.3 Consider consultation

We should always seek to consult individuals, their representatives and stakeholders, unless there is a good reason not to. In either case the results should be recorded, especially if the DPIA decision is at odds with the view of individuals.

If the DPIA covers the processing of new data processing activities we should design and implement a consultation process covering all of the major stakeholders, including data subjects. This might also involve a public consultation, targeted research or market research with targeted demographic groups for their views.

Think: Dp we need to consult anyone else?

Any decision to not consult should be recorded with a clear explanation of the reasons.

6.4 Assess the need for proportionality

Do our plans help achieve our purpose?

Do they ensure data protection compliance? There are many questions we could ask we could ask about our specific project, but the very minimum we should ask is

- What is our lawful basis?
- Are we processing special category data?
- How do we ensure the data subject's rights are upheld?
- Is there any other reasonable way to achieve the same result?

6.5 Identify and assess the risks

There is no explicit definition of 'risk' in the GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. Article 35 says that a DPIA must consider "risks to the rights and freedoms of natural persons". This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

Although the focus is on potential harm to individuals, the approach should also look at the possibility for more intangible harms like "significant economic or social disadvantage".

We should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).

The GDPR is clear that assessing the level of risk involves looking at both the **likelihood** and the **severity** of the potential harm, whether physical, emotional or material.

We must make an 'objective assessment' of the risks. We might find it helpful to use a structured matrix to think about likelihood and severity of risks. The matrix below is based on the council's corporate risk matrix and should be used wherever circumstances permit

LIKELIHOOD	IMPACT					
		Trivial **(1)**	Minor **(2)**	Moderate **(3)**	Major **(4)**	Severe **(5)**
	Almost Certain **(5)**	**Low**	**Medium**	**High**	**High**	**High**
	Likely **(4)**	**Low**	**Low**	**Medium**	**High**	**High**
	Possible **(3)**	**Low**	**Low**	**Medium**	**Medium**	**High**
	Unlikely **(2)**	**Low**	**Low**	**Low**	**Low**	**Medium**
	Rare **(1)**	**Low**	**Low**	**Low**	**Low**	**Low**
Impact Score x Likelihood Score = Risk Rating						

We multiply the potential harmful 'Impact' by the 'Likelihood' of an event happening to arrive at a score of 1 (trivial & rare) to 25 (severe and almost certain)

- **GREEN** – A score of 8 or below. we still work to see if we can develop and implement and apply any solutions or mitigating actions to reduce the risk far as possible. Most green rated risks are acceptable and so focus should be placed on those with higher ratings. Even where a green RAG rating has been given at the risk/privacy identification stage, this risk is still assessed and recorded.
- **AMBER** – score 8 to 14. mitigating actions are always proposed and outcomes envisaged, before processing is approved. The aim is to reduce all risks to a green level (*acceptable)*, however there will be occasions when processing must take place for legal/best interest reasons. Some processing with risks may go ahead and may be accepted into the project. All solutions and mitigating actions must first be considered, tried and applied if possible.
- **RED** – 14 and above. indicates that either or both impact and/or likelihood scores are unacceptable. Complete solutions and mitigating actions would be required to bring both indicators down to an acceptable level. Some processing activities are eliminated at this point as the impact to individuals is considered too high risk to proceed.

6.6 Identify measures to mitigate the risks

Against each risk identified, record the source of that risk. We should then consider options for reducing that risk.

Record whether the measure would reduce or eliminate the risk. We can take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

We do not always have to eliminate every risk. However, if there is still a high risk, we must consult the ICO before we go ahead with the processing.

6.7 'Sign off' and record outcomes

We should record:

- what additional measures we plan to take;
- whether each risk has been eliminated, reduced, or accepted;

- the overall level of ‘residual risk’ after taking additional measures; and
- whether we need to consult the ICO.

As part of the sign-off process, we should ask the DPO to advise on whether the processing is compliant and can go ahead. If we decide not to follow their advice, but whatever we decide, we need to record our reasons.

We should also record any reasons for going against the views of individuals, data subjects or other consultees.

6.8 Integrate outcomes into the project plans

We must;

- integrate the outcomes of our DPIA back into the project plans.
- identify any action points and who is responsible for implementing them.
- use the usual project management process to ensure these are followed through.
- monitor the ongoing performance of the DPIA. We may need to cycle through the process again before our plans are finalised.

If we decide to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, we need to consult the ICO before we can go ahead with the processing. See “Consulting the ICO” for more information on the consultation process.

6.9 Keep the DPIA under review

We need to keep the DPIA under review. We may need to repeat the cycle if there is a substantial change to the nature, scope, context or purposes of our processing.

7. Consulting the ICO

When do we need to consult the ICO?

If we have carried out a DPIA that identifies a high risk to the data security and rights of individuals **and** we cannot take any measures to reduce this risk, we must consult the ICO. We cannot go ahead with the processing until we have done so.

The focus is on the ‘residual risk’ after any mitigating measures have been taken. If our DPIA identified a high risk, but we have taken measures to reduce this risk so that it is no longer a high risk, we do not need to consult the ICO.

8. Handling Personal Information

Process for monitoring compliance.

Overall monitoring will be the responsibility of the SIRO however, the Data Protection Officer role will be to provide regular reports and monitoring to the SIRO.

Monitoring will be through:

- Action Plans from DPIA;
- Risk Assessment Action Plans;
- Project Risk and Issues logs;
- Audit of DPIA process on an annual basis (SWAP)?;
- Audit of DPIA documentation.

Shortfalls identified will be discussed at the Information Risk Group. Action Plan(s) should be devised.

9. Cross reference with to other documents

ECHR or Human Rights Act Article 8
GDPR
Data Protection Act 2018
WP248
Common law duty of confidentiallity
Data Protection Policy
Freedom of Information Policy
Information Security Policy
Risk Management Policy and Procedures
(ETC)
All current policies and procedures are accessible on Sharepoint

10. Glossary and definitions

Accreditation of Information Assets – The screening questions and full scale DPIA will form part of the accreditation documentation for an Information Asset

DPIA – (Data Protection Impact Assessment) A risk technique advocated by the ICO to enable organisations to address privacy concerns and ensure appropriate safeguards are addressed and built in as projects or plans to develop existing information assets.

Dorset Council is the data controller under the GDPR

Data Controller is a person or an organisation who determines the purposes and the manner in which any personal data is processed.

Data Processor is any person who processes the data on behalf of the data controller. This includes the Council's Services Units.

Data Processing (in relation to information or data) is the collection, recording and/or holding the information and carrying out any actions using it.

Data Subject is an individual who is the subject of personal data

GDPR – The General Data Protection Regulation

Information Asset – An Information Asset is any data, processed by us. It is held in an electronic or hard copy/manual format. Therefore, we are the data controller.

Senior Information Risk Owner (SIRO) The SIRO for Dorset Council is the Joint Director for Corporate Services. He/she is responsible for identifying all risks to the information and making sure that appropriate procedures are in place so that those risks can be managed1.

Special Category Data – under the GDPR and Data Protection Act 2018 is data for example such as patient diagnosis, medical history, ethnicity, sex, religion.

11. review

This Process & procedure will be reviewed when necessary, to take into account changes in the requirements of processing DPIAs within the council and changes in current legislation and best practice.

12. Authorisation & Recording

It is important to record decisions.

All stages and aspects of a Data Protection Impact Assessment are recorded and retained for the lifetime of the project plus 6 years after the project's end date. These may be referenced or reused should a similar project or technology be applied in the future.

The stages in the DPIA aim to demonstrate that we are carrying out effective assessments when high risks to privacy are involved and that the security and privacy of personal data is one of our main priorities. Keeping records of all stages enables us to evidence that we have identified, assessed and mitigated at every stage and that all risks have been evaluated.

Where there is a requirement for us to send a copy of the DPIA report to the ICO, we do and await their authorisation to proceed before going ahead with any processing. Such disclosures include the full report, along with a summary of the project, risks and proposed solutions.

The finalised DPIA is authorised by the DPIA Lead, Information Asset Owner, SIRO and DPO and any other person, (eg. ICT lead) if required

There is a sample DPIA Authorisation checklist at Appendix 3

13. Appendix 1 - Screening Questions

We always carry out a DPIA if we plan to:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data or criminal offence data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.
- Use new technologies.
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Carry out profiling on a large scale.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision-making or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach.

We consider whether to do a DPIA if we plan to carry out any other:

- Evaluation or scoring.
- Automated decision-making with significant effects.
- Systematic processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing involving preventing data subjects from exercising a right or using a service or contract.

We consider carrying out a DPIA in any major project involving the use of personal data. If we decide not to carry out a DPIA, **we document our reasons**.

We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing

14. Appendix 2 - DPIA process checklist

We always;

- describe the nature, scope, context and purposes of the processing.
- ask our data processors to help us understand and document their processing activities and identify any associated risks.
- consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- ask for the advice of our data protection officer.
- check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.
- do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.
- identify measures we can put in place to eliminate or reduce high risks.
- record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- implement the measures we identified, and integrate them into our project plan.
- consult the ICO before processing, if we cannot mitigate high risks.
- keep our DPIAs under review and revisit them when necessary.

15. Appendix 3 – DPIA Authorisation checklist

Name of DPIA Project Click or tap here to enter text.

DPIA Lead			
Name		Signature	
DPIA authorised	☐ Yes ☐ No	Date	Click or tap to enter a date.
Add additional text			

Information Asset Owner			
Name		Signature	
DPIA authorised	☐ Yes ☐ No	Date	Click or tap to enter a date.
Add additional text			

Senior Information Risk Owner			
Name		Signature	
DPIA authorised	☐ Yes ☐ No	Date	Click or tap to enter a date.
Add additional text			

Data Protection Officer			
Name		Signature	
DPIA authorised	☐ Yes ☐ No	Date	Click or tap to enter a date.
Add additional text			

Other (Job title)			
Name		Signature	
DPIA authorised	☐ Yes ☒ No	Date	Click or tap to enter a date.
Add additional text			

Data Protection Impact Assessment (DPIA) Guidance

Version Control			
Status	Choose an item.	Version	
Effective date	Click or tap to enter a date.	Authorised by	
Revision due	Click or tap to enter a date.	Revised by	

Contents

1. Introduction

In following this process and ensuring that Data Protection Officer are notified and involved from the initial conception of the project we can provide assurance the Council's information is being handled in a secure and responsible way and complies with legislation.
Note: The DPIA is only applicable where the proposed new project/system/process or proposed change to a system/process is to use personal confidential or special category (sensitive) data, or significantly change the way in which personal data is handled

Data Subjects have rights laid down in the GDPR. Those rights include the right;

- to be informed that processing of personal data is being undertaken of access to one's personal data to rectification of personal data
- to erasure ('the right to be forgotten')
- to restriction of processing.
- to be notified of rectified, erased or restricted processing.
- to data portability
- to object to data processing
- to not be subjected to automated decision making

Further, we are required to take appropriate technical and organisational security measures to safeguard personal information in all office and public spaces, on Council owned equipment, including mobile devices, and staff owned personal mobile devices (e.g. laptops, ipads, iphones) which are used to share and process personal and sensitive information.

Ensure that personal information is not transferred abroad without suitable safeguards

Special Categories' of Personal Data

The GDPR requires that controlling or processing special categories of personal data without a lawful basis, or explicit consent for one or more specified purposes is prohibited. Those special categories are:

a) Racial or ethnic origin
b) Political opinions
c) Religious or philosophical beliefs
d) Trade union membership
e) Genetic data & biometric data for the purpose of uniquely identifying an individual
f) Health
g) Sex life or sexual orientation

additionally

h) Criminal convictions and offences require control of official authority.

Link to GDPR Principles

GDPR Article 5 Principle 1 (a), - **Lawfulness, fairness** and **transparency** - Personal data shall be processed fairly and lawfully

Have we identified the purpose of the project?

- What is the legal basis for processing?
- How will individuals be told about the use of their personal data?
- Do we need to amend our privacy notices?
- If we are relying on consent to process personal data, how will this be collected and what will we do if it is withheld or withdrawn?

GDPR Article 5, Principle 1 (b) - **Purpose limitation**. Personal data shall be collected for specified explicit and legitimate purposes…

- Does our project plan cover all of the purposes for processing personal data?
- Have potential new purposes been identified as the scope of the project expands?

GDPR Article 5, Principle 1 (c) – **Data minimisation** - Personal data shall be adequate, relevant and limited to what is necessary….

- Is the data we are using of good enough quality for the purposes it is used for?
- Which personal data could we not use, without compromising the needs of the project?

GDPR Article 5, Principle 1 (d) - **Accuracy** - Personal data shall be accurate and, where necessary, kept up to date…

- If we are procuring new software does it allow us to amend data when necessary?
- How are we ensuring that personal data obtained from individuals or other organisations is accurate?
- How will we maintain accuracy over time?

GDPR Article 5, Principle 1 (e) - **Storage Limitation** - kept for no longer than necessary for that purpose…

- What retention periods are applicable for the personal data we will be processing?
- Are we procuring software which will allow us to delete information in line with our retention periods?
- Could we set the software to automatically delete information on its disposal date?

GDPR Article 5, Principle 1 (f) – **Integrity** and **Confidentiality** - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to, personal data.

- Do the new systems provide adequate protection against the security risks we have identified?
- What training and instructions are necessary to ensure that all staff know how to operate a new system securely?
- If we are transferring data, how will this be done securely?
- How will we protect the data at rest?

GDPR Article 3 – Territorial Scope - not transferred to a country or territory outside the European Union (EU) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Will the project require us to transfer data outside of the EU?
- If we will be making transfers, how will we ensure that the data is adequately protected?

GDPR Articles 12 – 23 - Individual rights - processed in accordance with the rights of data subjects

- Do we need **consent** of the individual to process this information?
- How can we take account of **objections** to the processing?
- Will the systems we are putting in place allow us to respond to **subject access requests** more easily?
- Are we processing information of **children aged 13-16**?
- If the project involves **marketing**, have we got a process for individuals to opt IN to their information being used for that purpose?
- How do we consider and action requests to **cease processing**?
- How do we consider and action requests to **delete** an individual's information?

Consider **The Human Rights Act 1998**:

- Will our actions interfere with the right to privacy under Article 8?
- Have we identified the social need and aims of the project?
- Are our actions a proportionate response to the social need?

Consider **The Common Law Duty of Confidentiality:**

- Will the information be given under a Duty of Confidentiality?

We must consider a DPIA for any processing of personal data '**likely to result in a high risk**'' to the rights and freedoms of individuals. There is no definition of 'high risk' but we need to consider the likelihood and severity of any potential breach to those rights and freedoms.

2. What is a data protection impact assessment?

Data protection impact assessments a tool which can help the council identify the most effective way to comply with our data protection obligations and meet Data Subjects rights and expectations of privacy.
Consultation with stakeholders may give them assurance that we are processing data competently and with their best interests at heart
An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and potential damage to reputation, which might otherwise occur.
The ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach.
See the ICO's detailed guidance on data protection impact assessments for good practice advice.
The council must comply with the GDPR, the Data Protection Act 2018 and other UK privacy laws when we process such information. The council has drafted this policy following the ICO DPIA good practice guidance and screening questions outlined in

3. What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller (see Article 6 GDPR).
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that we comply.
- A DPIA can address more than one processing activity

The relevant provisions in the GDPR – see Articles 35, 36 and 83 and Recitals 84, 89 and 96

4. Do we need to do a DPIA?

We should carry out a DPIA if we plan any new data processing activity likely to result in a high risk to peoples' personal data

The **GDPR** says we **Must** do a DPIA if we plan to:

- use systematic and extensive profiling with significant effects;
- process special-category or criminal-offence data on a large scale; or

- systematically monitor publicly accessible places on a large scale

The ICO says we **Must** do DPIA

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach

We should also think carefully about doing a DPIA for any other processing that involves:

- large scale processing,
- profiling or monitoring,
- decisions on access to services or opportunities,
- sensitive data or vulnerable individuals.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data. You can use or adapt the checklists to help you carry out this screening exercise.

We may not have to carry out a DPIA if:

We are processing on the basis of **legal obligation** or **public task.** However, this exception only applies if:

- we have a clear statutory basis for the processing;
- the legal provision or a statutory code specifically provides for and regulates the processing operation in question;
- we are not subject to other obligations to complete DPIAs, such as mandatory minimum measures required by Cabinet Office for consideration of information governance risks or requirements derived from specific legislation, such as Digital Economy Act 2017; or
- a data protection risk assessment was carried out as part of the impact assessment when the legislation was adopted.

This may not always be clear, and in the absence of any clear and authoritative statement on whether such an assessment was conducted the ICO recommends that we err on the side of caution and conduct a DPIA to ensure we consider how best to mitigate any high risk.

- We have already done a substantially **similar** DPIA. We need to be confident that we can demonstrate that the nature, scope, context and purposes of the processing are all similar.

- The ICO issues a list of processing operations which do not require a DPIA**.** The ICO has the power to establish this type of list, but has not done so yet.

5. Who should be involved?

If the screening questions indicate that an assessment is required, the DPIA Team Lead will assess the processing operations that will be involved in the DPIA (*using the positively answered screening questions*) and decide if any further team members are required. ***This includes choosing specific team members who: -***

- Understand the project's aims and the organisation's objectives
- Authority to influence the design and development of the project and participate in decisions
- Expertise in data protection and compliance matters
- Ability to assess and suggest solutions to risks and develop mitigating actions
- Ability to communicate effectively with stakeholders and management
- The DPIA Team Lead can at any point in the DPIA process, engage other members to assist in specific areas as they deem fit or necessary.

The list below is the very minimum of persons who should be involved in a DPIA. In most cases far more will be.

- A Lead Officer
  This is the person who will carry out the DPIA and should have sufficient responsibility and authority to be able to carry through the DPIA requirements. This person will also be the first contact with the 'Risk and Resilience' team etc
- Information Asset Owner
  The person who is currently or will be responsible for the Information Asset. This may be the same person as the Lead Officer
- Data Protection Officer
  Must be involved in all DPIAs. The DPO will offer advice and guidance in line with current best practice and legislation
- ICT data security
  Especially if the asset is an IT one

There may be others involved depending on the circumstances

- Data Subjects
  Should be consulted where there is a need
- Internal and external stakeholders
  People who may process the data or rely on it to perform their own legitimate duties and tasks. For example, the health service my need to use some of our data in the best interests of their patients. The police may need to process some of our data to use in safeguarding cases. We should be aware of their requirements and the data subjects' responses to this proposed third party access
- Data processors
  Third parties, possibly subcontractors or providers of systems we use to host our service user's or employees' data
- Legal services
  Who may need to be assured that the information asset complies with legal requirements, or may need include or update contractual terms to assure GDPR compliance

This list is NOT exhaustive.

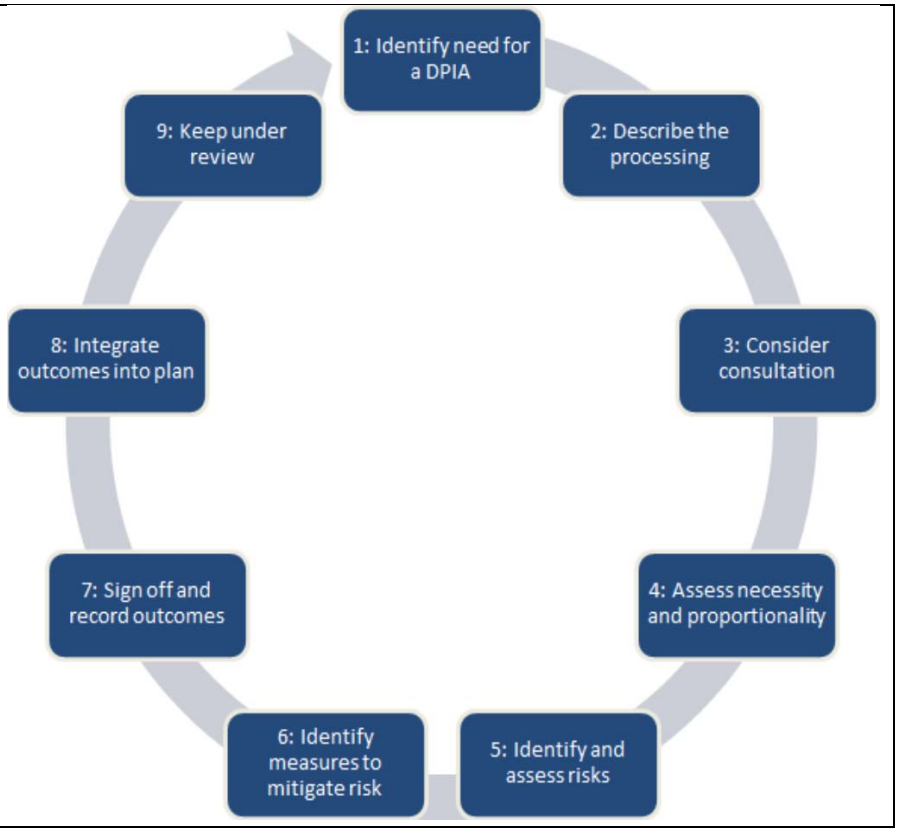
DPIA guidance is provided for staff members by the Data Protection Officer, as part of the Information Asset Owner training.
The Data Protection Officer is also responsible for ensuring support and guidance is given when staff members are required to fill out the DPIA.

6. DPIA Stages

A DPIA is an iterative process. It should be constantly reviewed. A DPIA is designed to be flexible and scalable, with time and resources allocated to fit the approach to the risks

A DPIA should be done in stages, to ensure that all aspects are reviewed and documented.

Identify the need for a DPIA
Describe the processing
Consider consultation
Assess the necessity for proportionality
Identify and assess risks
Identify measures to mitigate the risks
Sign off and record outcomes
Integrate outcomes into the project plan
Keep our DPIA under review



The following process **must** be followed:

The lead officer for the DPIA should work closely with the Information Asset Owner is responsible for ensuring the DPIA is completed and that the DPIA is carried out with support and guidance from other individuals as relevant, i.e. The Data Protection Officer, ICT etc.

6.1 Identify the need for a DPIA (Screening questions)

Not all processing needs a DPIA. There are some screening questions that can help us to decide. These questions are not exhaustive. The ICO says we should always consult our Data Protection Officer if we are unsure.

Always carry out a DPIA if we

- **process data systematically or as a matter of course.**
- **begin any major new project involving personal data**

- **process special category data (the old "sensitive personal data") on a large scale or any data about criminal convictions.**
  See "introduction" for the list of special category data
- **systematically monitor a publicly accessible place on a large scale.**
  This might be CCTV, ANPR cameras, body mounted cameras etc
- **use new technologies.**
  Taken together with 'biometrics' (below), it is especially important to consider how privacy will be respected. Fingerprint scanners on phone or PCs or facial recognition software for identification purposes combined with CCTV would indicate a high need for a DPIA
- **use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit, especially on a large scale.**
  Do we use a scoring system to allocate benefits? If the scoring system is just to indicate something, that's fine, but a decision should not be made simply on the basis of a score without human intervention.
- might **refuse or deny a 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.
- **process biometric or genetic data.**
  Any new 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 should attract a DPIA
- **combine, compare or match data from multiple sources.**
  Data that could not previously identify and individual might make it easier when combined with other data sets.
  It is also wrong to use data for purposes other than those for which it was originally collected. It is rare for combined data to meet this criteria
- **process personal data without providing a privacy notice directly to the individual.**
  The vast majority of data the council processes will have a privacy notice based on the contents of the Information Asset register. If this is a new form of processing, and entry on the IAR will need to be considered as well as the DPIA
- **process personal data in a way which involves tracking individuals' online or offline location or behaviour.**
  Includes CCTV, GPS or other geolocation tools, WiFi or Bluetooth tracking etc
- **process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.**
  Data collected from or about children (or any vulnerable person) should be treated especially carefully
- **process personal data which could result in a risk of physical harm in the event of a security breach.**
  Where the processing is of such a nature that a personal data breach could jeopardise the health or safety of individuals
- conduct **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 would prove impossible or involve disproportionate effort.

Consider whether to do a DPIA if we plan to carry out any other:

- Evaluation or scoring.
- Automated decision-making with significant effects.
- Systematic processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing involving preventing data subjects from exercising a right or using a service or contract.

We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

- Especially if we use existing data for new or novel reasons that could not have been foreseen at the time of collection and would not be expected by the data subject now

If we decide not to carry out a DPIA, we should document our reasons.

6.2 Describe the processing

How do we use the data. We need to look at the;

Nature of the processing - what we plan to do with the personal data; and

- how we collect the data;
- how we store the data;
- how we use the data (including any potential future uses);
- who has access to the data;
- who we share the data with;
- whether we use any processors;
- retention periods;
- security measures;
- whether we are using any new technologies;
- whether we are using any novel types of processing; and
- which screening criteria we flagged as likely high risk

The scope of the processing - what the processing covers; and

- the nature of the personal data;
- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved; and
- the geographical area covered.

The context of the processing – internal and external factors affecting the data; The wider picture. Things that might affect expectations or outcomes

- the source of the data;
- the nature of our relationship with the individuals;
- the extent to which individuals have control over their data;
- the extent to which individuals are likely to expect the processing;
- whether they include children or other vulnerable people;
- any previous experience of this type of processing;

- any relevant advances in technology or security;
- any current issues of public concern; and
- in due course, whether we comply with any GDPR codes of conduct (once any have been approved under Article 40) or GDPR certification schemes.
- Whether we have considered and complied with relevant codes of practice.

The purpose of the processing – the reason why we would want to process the data.

- our legitimate interests, where relevant;
- the intended outcome for individuals; and
- the expected benefits for us or for society as a whole

6.3 Consider consultation

We should always seek to consult individuals, unless there is a good reason not to. In either case the results should be recorded, especially if the DPIA decision is at odds with the view of individuals.

If the DPIA covers the processing of new data processing activities we should design and implement a consultation process covering all of the major stakeholders, including data subjects. This might also involve a public consultation, targeted research or market research with targeted demographic groups for their views.

Consider consulting;

- ICT and the persons responsible for data security. Individuals who understand the initiative from a technical point of view and in terms of personal data processing
- Other internal stakeholders, especially those who may use the system or process the data.
- Legal services to review or implement new data sharing terms or update contracts
- Other data processors
- Individuals whose personal data will be processed by the new system or process
- Collaborative partners
- The suppliers of a system

Any decision to not consult should be recorded with a clear explanation of the reasons. Some examples of potential reasons to not consult may be.

- It might compromise confidentiality
- The consultation itself might have the potential to cause harm of distress
- It might be disproportionate and impractical

Consultation serves many purposes throughout the DPIA process, such as:

- Explaining the initiative to stakeholders.
- Establishing the privacy concerns of stakeholders.
- Explaining to stakeholders how the DPIA process will be used within the initiative to manage privacy risks.
- Explaining identified controls to stakeholders.
- Soliciting suggestions for controls.
- Establishing current working practices that the initiative aims to update or replace.
- Establishing how the new system or process is likely to be used in practice and in the case of general purpose facilities, their likely purpose.

In cases where the impact of a risk identified at section 6.5 is assessed to be either severe or major and likelihood is assessed to be either likely or very likely, the council's Data Protection Officer must be consulted. If any risk remains at this level after the implementation of controls, the council may be required to consult the Information Commissioner's Office

6.4 Assess the need for proportionality

We should consider:

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

The Article 29 guidelines also say we should include how we ensure data protection compliance, which are a good measure of necessity and proportionality. In particular, we should include relevant details of:

- the lawful basis for the processing;
- how to prevent function creep; One function turns into another that was not envisaged at the start
- how we implement and support individuals' rights;
- how we intend to ensure data quality, including accuracy
- how we intend to ensure data minimisation;
- how we intend to provide privacy information to individuals, including SAR's and Business as Usual;
- measures to ensure our processors comply, including any third party data hosts and developers

6.5 Identify and assess the risks

There is no explicit definition of 'risk' in the GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. Article 35 says that a DPIA must consider "risks to the rights and freedoms of natural persons". This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

Record the identified risks in the DPIA template. This forms the core of the DPIA process. The aim is to compile a comprehensive list of all of the privacy risks associated with the initiative, whether or not the risks require action.

For each privacy risk identified, the following should be recorded:

- A unique identifier
- A description of the risk
- An assessment of the impact of the risk (severe, major, moderate, minor, trivial)
- An assessment of the likelihood of the risk (almost certain, likely, possible, unlikely, rare)

The key provision here is Recital 75, which links risk to the concept of potential harm or damage to individuals:

> *"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data…"*

The focus is therefore on any potential harm to individuals. However, the risk-based approach is not just about actual damage and should also look at the possibility for more intangible harms like "significant economic or social disadvantage".

The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if our intended processing leads to a loss of public trust.

Risks will usually fall into one of three categories:

- ***Risks to Individuals*** - Any risk that affects a data subject, their data, their privacy or their rights is classed as a risk to an individual. Inadequate disclosure controls, consent issues, processing purposes and surveillance methods are just a few of the issues that may result in risks to individuals.
- ***Compliance Risks*** - These can arise where the assessment response indicates that a breach of laws, legislation and/or regulations will occur if the processing goes ahead. This can include non-compliance with the GDPR, PECR or human rights legislation.
- ***Corporate Risks*** - Risks that will affect the business, including reputation, revenue, fines and sanctions. These will mainly arise where the initial collection, consent, disclosures, sharing and storage of the personal information have not been complied with or where record keeping is ineffective.

We should also consider the council's own corporate risks, such as the impact of regulatory action, reputational damage or loss of public trust.

A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

Consider the potential impact on individuals and any harm or damage that might be caused by our processing – whether physical, emotional or material. In particular look at whether the processing could possibly contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- reidentification of pseudonymised data; or
- any other significant economic or social disadvantage

We should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).

To assess whether the risk is a high risk, we need to consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

We must make an 'objective assessment' of the risks. We might find it helpful to use a structured matrix to think about likelihood and severity of risks. The matrix below is based on the council's corporate risk matrix and should be used wherever circumstances permit

		IMPACT				
		Trivial (1)	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Severe (5)**

	Almost Certain (5)	Low	Medium	High	High	High
	Likely (4)	Low	Low	Medium	High	High
	Possible (3)	Low	Low	Medium	Medium	High
	Unlikely (2)	Low	Low	Low	Low	Medium
	Rare (1)	Low	Low	Low	Low	Low
Impact Score x Likelihood Score = Risk Rating						

- **GREEN** - we still work to see if we can develop and implement any solutions or mitigating actions that can be applied to reduce the risk far as possible. However, most green rated risks are acceptable and so focus should be placed on those with higher ratings. Even where a green rating has been given at the risk/privacy identification stage, this risk should still be added to the template for continuity and to ensure that all risks have been recorded and assessed.
- **AMBER** - mitigating actions are always proposed and outcomes envisaged, before processing is approved. The aim is to reduce all risks to a green level (*acceptable)*, however there will be occasions when processing must take place for legal/best interest reasons and so some processing with risks will go ahead and must be accepted into the project. All solutions and mitigating actions must be considered and applied if possible.
- **RED** - indicates that either or both impact and/or likelihood scores are unacceptable and that complete solutions and mitigating actions would be required to bring both indicators down to an acceptable level. Some processing activities are eliminated at this point as the impact to individuals is considered too high risk to proceed.

6.6 Identify measures to mitigate the risks

Identify controls to mitigate the risks and record them in the DPIA template. The aim is to identify sufficient controls to eliminate each of the risks identified in 6.5, or to reduce them to a level which is acceptable to the council. For some identified risks, no controls may be required because the likelihood is so low and/or the impact so small that the risks are acceptable to the council

Against each risk identified, record the source of that risk. We should then consider options for reducing that risk. For example:

- deciding not to collect certain types of data;
- additional terms and conditions in a contract;
- a privacy notice or making changes to and existing privacy notice;
- documented operational procedures, writing internal guidance or processes to avoid risks;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures or disabling certain product features;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- using a different technology;
- putting clear data sharing agreements into place;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

This is not an exhaustive list, and we may be able to devise other ways to help reduce or avoid the risks. Ask the DPO for advice.

Record whether the measure would reduce or eliminate the risk. We can take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

6.7 Sign off and record outcomes

The risks then need to be accepted by an appropriate individual. Normally this should be the information asset owner or their nominated delegate,

The individual who signs off the risks should have a clear understanding of the initiative, particularly the privacy risks and how the controls address them. If any risk has not been reduced to an acceptable level after implementation of the controls identified in 6.6, additional controls will need to be identified and steps will need to be repeated.

We should then record:

- what additional measures we plan to take;
- whether each risk has been eliminated, reduced, or accepted;
- the overall level of 'residual risk' after taking additional measures; and
- whether we need to consult the ICO.

We do not always have to eliminate every risk. We may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. However, if there is still a high risk, we need to consult the ICO before we can go ahead with the processing.

As part of the sign-off process, we should ask the DPO to advise on whether the processing is compliant and can go ahead. If we decide not to follow their advice, but whatever we decide, we need to record our reasons.

We should also record any reasons for going against the views of individuals data subjects or other consultees.

6.8 Integrate outcomes into the project plans

After the controls have been implemented, re-assess the risks and record the outcome in the DPIA template.

We must

- integrate the outcomes of our DPIA back into the project plans.
- identify any action points and who is responsible for implementing them.
- use the usual project management process to ensure these are followed through.
- monitor the ongoing performance of the DPIA. We may need to cycle through the process again before our plans are finalised.

If we have decided to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, we need to consult the ICO before we can go ahead with the processing. See the next section for more information on this consultation process.

Under most circumstances, the council will publish the DPIA to aid transparency and accountability. This could help foster trust in our processing activities, and improve individuals' ability to exercise their rights. If we are concerned that publication might reveal commercially sensitive information, undermine security or cause other risks, we should consider whether we can redact (black out) or remove sensitive details, or publish a summary. We also need to consider our Freedom of Information obligations, as privacy impact assessments are included in the definition documents for publication schemes for many public authorities.

6.9 Keep the DPIA under review

We need to keep the DPIA under review. We may need to repeat it if there is a substantial change to the nature, scope, context or purposes of our processing.

It is good practice to publish our DPIA to aid transparency and accountability. We also need to consider our freedom of information obligations. DPIAs are included in the definition documents for publication schemes for public authorities.

7. Consulting the ICO

When do we need to consult the ICO?

If we have carried out a DPIA that identifies a high risk, and we cannot take any measures to reduce this risk, we need to consult the ICO. We cannot go ahead with the processing until we have done so.

The focus is on the 'residual risk' after any mitigating measures have been taken. If our DPIA identified a high risk, but we have taken measures to reduce this risk so that it is no longer a high risk, we do not need to consult the ICO.

The ICO is oblige to respond in writing within eight weeks although that period can be extended a further six weeks in exceptional circumstances

8. Handling Personal Information

Process for monitoring compliance.

Overall monitoring will be the responsibility of the SIRO however, the Data Protection Officer role will be to provide regular reports and monitoring to the SIRO.

Monitoring will be through:

- Action Plans from DPIA;
- Risk Assessment Action Plans;
- Project Risk and Issues logs;
- Audit of DPIA process on an annual basis (SWAP)?;
- Audit of DPIA documentation.

Shortfalls identified will be discussed at the Information Risk Group? and Action Plan(s) devised.

9. CROSS REFERENCE TO OTHER PROCEDURAL DOCUMENTS

Data Protection Policy
Freedom of Information Policy
Information Security Policy
Risk Management Policy and Procedures
(ETC)
All current policies and procedures are accessible on Sharepoint

10. Glossary and definitions

Accreditation of Information Assets – The screening questions and full scale DPIA will form part of the accreditation documentation for an Information Asset

Information Asset – An Information Asset is any data, processed by us. It is held in an electronic or hard copy/manual format. Therefore, we are the data controller.
GDPR – The General Data Protection Regulation
DPIA – (Data Protection Impact Assessment) A risk technique advocated by the ICO to enable organisations to address privacy concerns and ensure appropriate safeguards are addressed and built in as projects or plans to develop existing information assets.
Dorset Council is the data controller under the GDPR
Data Subject is an individual who is the subject of personal data
Data Controller is a person or an organisation who determines the purposes and the manner in which any personal data is processed.
A **Data Processor** is any person who processes the data on behalf of the data controller. This includes the Council's Services Units.
Data Processing (in relation to information or data) is the collection, recording and/or holding the information and carrying out any actions using it.
Senior Information Risk Owner (SIRO) The SIRO for Dorset Council is the Joint Director for Corporate Services. He/she is responsible for identifying all risks to the information and making sure that appropriate procedures are in place so that those risks can be managed1.
Special Category Data – under the GDPR and Data Protection Act 2018 is data for example such as patient diagnosis, medical history, ethnicity, sex, religion.

11. review

This Process & procedure will be reviewed when necessary, to take into account changes in the requirements of processing DPIAs within the council and changes in current legislation and best practice.

12. Authorisation & Recording

It is important to record decisions.

All stages and aspects of a Data Protection Impact Assessment are recorded and retained for 6 years after the project implementation date. These may be referenced or reused should a similar project or technology be utilised in the future.

The stages in the DPIA aim to demonstrate that we are carrying out effective assessments when high risks to privacy are involved and that the security and privacy of personal data is one of our main priorities. Keeping records of all stages enables us to evidence that we have identified, assessed and mitigated at every stage and that all risks have been evaluated.

Where there is a requirement for us to send a copy of the DPIA report to the ICO, we do this within the deadlines and await their authorisation to proceed before going ahead with any processing. Such disclosures include the full report, along with a summary of the project, risks and proposed solutions.

The finalised DPIA is authorised by the DPIA Lead, Information Asset Owner, SIRO and DPO and any other person, (eg. ICT lead) if required

There is a sample DPIA Authorisation checklist at Appendix 3

13. Appendix 1 - Screening Questions

We always carry out a DPIA if we plan to:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data or criminal offence data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.
- Use new technologies.
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Carry out profiling on a large scale.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision-making or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach.

We consider whether to do a DPIA if we plan to carry out any other:

- Evaluation or scoring.
- Automated decision-making with significant effects.
- Systematic processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing involving preventing data subjects from exercising a right or using a service or contract.

We consider carrying out a DPIA in any major project involving the use of personal data. If we decide not to carry out a DPIA, **we document our reasons**.

We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing

14. Appendix 2 - DPIA process checklist

We always;

- describe the nature, scope, context and purposes of the processing.
- ask our data processors to help us understand and document their processing activities and identify any associated risks.
- consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- ask for the advice of our data protection officer.
- check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.
- do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.
- identify measures we can put in place to eliminate or reduce high risks.
- record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- implement the measures we identified, and integrate them into our project plan.
- consult the ICO before processing, if we cannot mitigate high risks.
- keep our DPIAs under review and revisit them when necessary.

15. Appendix 3 – DPIA Authorisation checklist

Name of DPIA Project Click or tap here to enter text.

DPIA Lead - Remember who the lead should be			
Name		Signature	
DPIA authorised	☐ Yes ☐ No	Date	Click or tap to enter a date.
Add additional text			

Information Asset Owner			
Name		Signature	
DPIA authorised	☐ Yes ☐ No	Date	Click or tap to enter a date.
Add additional text			

Senior Information Risk Owner			
Name		Signature	
DPIA authorised	☐ Yes ☐ No	Date	Click or tap to enter a date.
Add additional text			

Data Protection Officer			
Name		Signature	
DPIA authorised	☐ Yes ☐ No	Date	Click or tap to enter a date.
Add additional text			

Other Job title			
Name		Signature	
DPIA authorised	☐ Yes ☑ No	Date	Click or tap to enter a date.
Add additional text			

Protected document. Pass = 0000

Shaping Dorset Council

Equality Impact Assessment (EqIA) Screening Template

Proposal / Brief Title	DPIA Policy
Date:	11 March 2019

Type of strategy, policy, project or service

Please tick one of the following:

Existing	☐	**Changing, update or revision***	☐
New or proposed	☑	**Other (please explain)**	☐

* Not every policy, service alignment or strategy change will require an EqIA. In some circumstances a new EqIA is not required:

- If the policy has had an EqIA last completed within a sovereign Council in the last 2 years
- If there is no significant change other than bringing policies together for Dorset Council with no change to the impact on people
- If the new policy aligns with existing EqIAs.

This report was created by

Name	James Fisher
Job Title	Information Services Team Leader
Email address	JFisher@dorset.gov.uk

1. Briefly describe the aims and objectives of the proposal.

The policy describes how the Council will conduct data protection impact assessments required under the GDPR.

2. What outcomes do we want to achieve?

Ensure data protection principles are fully considered and accounted for when procuring new systems, technology, undertaking corporate projects and making decisions with data protection implications.

3. Screening Questions	Yes	No	Please explain you answer.
Does this proposal plan to withdraw a service, activity or presence?		X	
Does this proposal plan to reduce a service, activity or presence?		X	
Does this proposal plan to introduce, review or change a		X	

policy, strategy or procedure that will have new or different impact on people?			
Does this proposal affect service users and/or customers, or the wider community?		x	The policy will help ensure that projects undertaken by the Council that may have an impact on customers fully considers data protection requirements.
Does this proposal affect employees?		x	
Will employees require training to deliver this proposal?		x	Guidance has been produced for staff completing a DPIA and Information Governance professionals will be available to support employees in the process.
Has any engagement/consultation been carried out?		x	
Are there any concerns at this stage which indicate that this proposal could have negative or unclear impacts on any of the protected characteristic group(s) below?			
Protected Characteristic	**Yes**	**No**	**Comments**
Age		**x**	
Disability		**x**	
Gender Identity		**x**	
Pregnancy & maternity		**x**	
Race & Ethnicity		**x**	
Religion & Belief		**x**	
Sex		**x**	
Sexual Orientation		**x**	
Marriage & Civil Partnership		**x**	
Carers		**x**	
Rural isolation		**x**	
Single parent families		**x**	
Poverty (social & economic deprivation		**x**	
Military families /veterans		**x**	
5. EqIA Screening and Declaration **If you have answered yes to any of the screening questions or any of the protected characteristic group(s), a full EqIA should be undertaken** **Complete the relevant declaration depending on your outcome:**			
EqIA to be completed	**Yes**	**EQIA not required**	**No**
Please briefly explain your answer.		Policy introduces no significant changes that require an EQIA and there are is no	

	potential impact on any groups with protected characteristics envisaged. **On what basis do you feel it is exempt?**		
Officer completing this Screening Template	**James Fisher**	**Date**	**11/03/2019**
Equality Lead		**Date**	
Diversity Action Group Chair		**Date**	
Review Date			

Please send this declaration to: shapingdorset@dorsetcc.gov.uk

Susan.Ward-Rice@dorsetcc.gov.uk