Data Protection Impact Assessment
Section 1: Project Brief

PROJECT:

PROJECT OWNER:

DATE:

1. Project Brief
What is the project?
What does it aim to achieve?
What are the benefits to the organisation?
What are the benefits to individuals?
What are the benefits to other parties?
Have you or anyone else done something similar?
What existing policies, procedures and laws will apply?
Whose privacy may be impacted?
What date will the project be implemented?

Data Protection Impact Assessment
Section 2: Processing Activities

2. Does the project involve any of the following?	Yes or No	Notes
Systematic and extensive profiling which is based on automated processing with significant effects.		
Processing of special category or criminal offence data on a large scale.		
Systematic monitoring of publicly accessible places on a large scale.		
Use of technology that is new to the service or a change in how an existing system is being used.		*Please provide details of what changes are proposed.*
Use of profiling or special category data to decide on access to services which is based on any extent of automated decision-making.		
Profiling of individuals on a large scale.		
Processing of biometric data.		
Processing of genetic data.		
Matching (comparing two or more sets) of data or combining datasets from different sources.		
Collecting personal data from a source other than the individual without providing them with a privacy notice (invisible processing).		
Tracking individuals' location or behaviour, including but not limited to the online environment.		
Profiling children (up to the age of 18) or targeting marketing or online services at them.		*Please confirm the age of any children being targeted.*
Processing data that might endanger the individual's physical health or safety in the event of a security breach.		
Collecting personal data for a major project		
Large scale processing of personal data.		
Profiling or monitoring.		
Making decisions about whether individuals can access services or opportunities.		
Sensitive data or vulnerable individuals.		
Communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.		
Sharing data between services.		
If you have not ticked any of the above, record the reasons why a DPIA is not needed and/or any issues that need to be considered below.		

Data Protection Impact Assessment
Section 3: Information Flows

3. Describe the collection, use and deletion of personal data			
What personal data will you collect? *Tick all that apply*			
Name ☐	Address ☐	Email address ☐	Financial data ☐
Age data ☐	Camera images ☐	Race ☐	Ethnic origin ☐
Political data ☐	Religion ☐	Trade union membership ☐	Genetic data ☐
Biometric data ☐	Health data ☐	Sex life ☐	Sexual orientation ☐
Other: *(please list categories / fields being collected)*			
Approximately how many individuals are likely to be affected by the project?			
How will you be collecting the data? *Online/paper forms, face-to-face, telephone, etc.…*			
Will you be collecting information directly from the individual or a third party?			
Is a privacy notice already in place covering this activity? *Please provide a copy.*			
Please explain what you will do with the data once it has been received? *Logged on a system, passed to someone else etc.…*			
Who will have access to the data? *Including particular job roles or contractors* etc...			
How and where will the data be stored?			
How long will the data retained for?			
How will the data be deleted?			

Data Protection Impact Assessment
Section 4: Lawful Basis

4. Initial assessment of lawful basis for processing
Before you can proceed, you must have a lawful basis for processing personal data. You will need to identify which of the lawful bases, as set out in the General Data Protection Regulations, applies to your processing activity.
Either a: If the project involves collecting **new** categories of data that you have not collected before, identify the lawful basis for processing: Lawful basis: **Choose an item.** If you are processing special category data, you will need to identify an additional lawful basis from the following: **Choose an item.** Comments:
Or b: If the project involves collecting **existing** categories of data in a different way to how it is collected currently, identify the lawful basis for processing from the Record of Processing Activity (ROPA). Lawful basis for existing data: Choose an item. If you are processing special category data, you will need to identify an additional lawful basis from the following: Choose an item. c: If the project involves using **existing data for a new purpose** identify the lawful basis for the new purpose and consider whether the new purpose is permitted. Lawful basis for new purpose: Choose an item. If you are processing special category data, you will need to identify an additional lawful basis from the following: Choose an item. ***Notes for Performance & Governance Team. Either:*** *1) Assess compatibility of original purpose with new purpose:* *a) Is the new purpose permitted by law?* *b) Is there a link between the purposes for original processing and the purposes of intended further processing?* *c) Would it be reasonable for data subjects to expect their data to be used in this way?* *d) What is the nature of the personal data?* *e) What are the consequences of the intended further processing for data subjects?* *f) Are there appropriate safeguards in both the original and intended further processing operations?* ***Or:*** *2) Have the data subjects given their consent to use the data for a new purpose?* ***Or:*** *3) Does the processing constitute a necessary and proportionate measure to safeguard important objectives of general public interest?*

Data Protection Impact Assessment
Section 5: Initial view of risks

5. Initial view of risks	
Are there any potential issues in relation to the data protection principles and rights below? See glossary pages 10 & 11	
Processing personal data in a way that is lawful, fair and transparent.	
Processing personal data for a specified and limited purpose.	
Processing only the minimum amount of personal data needed.	
Making sure personal data is accurate and up to date.	
Keeping personal data for no longer than necessary	
Putting appropriate security measures in place to protect personal data.	
Informing individuals about how their personal data is being used.	
Giving individuals access to their personal data when required.	
Rectifying inaccurate personal data about individuals when required.	
Erasing personal data about individuals when required.	
Restricting how an individual's personal data is used, if required.	
Providing individuals with their personal data in a way that allows them to reuse it for their own purposes (where applicable).	
Responding to requests from individuals who object to their personal data being processed.	
Responding to a requests for an automated decision to be reviewed by a member of staff (where applicable)	
Other rights in the Human Rights Act etc.…	
On which aspects of the project should a DPIA focus? *(to be reviewed by the Performance and Governance Team once the service has completed the template).*	

Data Protection Impact Assessment
Section 6: Risk Assessment

6. Risk assessment				
No.	**Why does the risk arise?**	**Potential Compliance Risk**	**Level of Risk**	**Further assessment**
1		Principles: Choose an item. Rights: Choose an item.		
2		Principles: Choose an item. Rights: Choose an item.		
3		Principles: Choose an item. Rights: Choose an item.		
4		Principles: Choose an item. Rights: Choose an item.		
5		Principles: Choose an item. Rights: Choose an item.		

Data Protection Impact Assessment
Section 7: Risk Solutions

7. Solutions						
No.	**Agreed Solution**	**Review of risk**	**Evaluation/ Comments**	**Responsible Officer/Sign Off**	**Date agreed**	**Date to be in place**
1		Choose an item.				
2		Choose an item.				
3		Choose an item.				
4		Choose an item.				
5		Choose an item.				
6		Choose an item.				

Data Protection Impact Assessment
Section 8: Stakeholders

8. Stakeholders		
Record a note of any discussions with relevant individuals below.		
Corporate Governance		
Name	**Date Discussed**	**Notes**
Digital Services		
Name	**Date Discussed**	**Notes**
MKS ICT		
Name	**Date Discussed**	**Notes**
MKS Legal		
Name	**Date Discussed**	**Notes**
Other		
Name	**Date Discussed**	**Notes**

Please send this document to the Policy and InformationTeam at Dataprotectionofficer@maidstone.gov.uk for review and approval by the Data Protection Officer (DPO). Please do not start collecting any personal data until you have received confirmation that this assessment has been approved by the DPO.

Data Protection Impact Assessment
Section 9: Action Plan and Sign Off

9. Action Plan *Corporate Governance Officer to record a list of actions to be included in quarterly performance monitoring.*	
Action	**Responsible Officer**

10. Data Protection Officer sign off		
Name	**Note of any risks to be reported to the Information Governance Forum**	**Date**

Glossary

Automated decision-making: making a decision solely by automated means without any human involvement.

Biometric data: specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person e.g. workplace access systems, identity verification or access control.

Genetic data: inherited or acquired characteristics of an individual which result from the analysis of a biological sample.

Large scale: taking into account the number of individuals concerned, the volume of data, variety of data, duration of processing and geographical extent of the processing.

Monitoring: automated analysis or predicting of behaviour, location, movements, reliability, interests, personal preferences, health, economic situation, performance.

Profiling: automated processing of information to evaluate certain things about an individual

Special category: data about race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, sexual orientation.

Vulnerable individuals: who, for whatever reason, may find it difficult to understand how their information is used.

Lawful basis for processing

Consent: the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Performance of a contract: processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Compliance with a legal obligation: processing is necessary for compliance with a legal obligation to which the Council is subject.

Vital interests: processing is necessary in order to protect the vital interests of the data subject or of another natural person.

Task in the public interest: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council.

Legitimate interests: processing is necessary for the purposes of the legitimate interests pursued by the Council or by a third party.

Lawful basis for processing (special category)

Explicit consent: the data subject has given explicit consent to the processing for one or more specified purposes.

Employment and social protection law: necessary for the purposes of carrying out the obligations and exercising specific rights of the Council or of the data subject in the field of employment and social security and social protection law.

Vital interests: necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

Legitimate activities: carried out in the course of legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.

Data made public by the data subject: relates to personal data which are manifestly made public by the data subject.

Legal claims: necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Substantial public interest: necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued.

Occupational medicine: necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

Public health: necessary for reasons of public interest in the area of public health.

Archiving purposes: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Glossary

Information Rights

The right to be informed – Individuals have the right to be given fair processing information, usually through privacy notices. This must be given in clear, plain English, free of charge, at the time the data is obtained.

The right of access – Individuals have a right to access their personal data, and some other supplementary information. We should be able to provide the information in a commonly used electronic format, or in a hard copy. Information should be easily accessible and collatable.

The right to rectification – Individuals have the right to have personal data rectified if it is inaccurate or incomplete. We must also inform any third parties with whom we have shared the data.

Right to erasure – Individuals have the right to request data is erased, and to prevent processing in certain circumstances. We must inform any third parties with whom we have shared the data.

Right to restrict processing – Individuals can also block or suppress processing of their data. We may still store it, but cannot process it further. We can also retain enough information as required, to ensure processing is restricted in the future.

Right to data portability – Data must be supplied in a commonly used and machine readable format such as a CSV file, that enables other organisations to use the data. This applies to data processed based on consent, or for the performance of a contract.

Right to object to processing – Individuals have the right to object to processing of data, but it must be on grounds relating to their own situation. We must stop processing the data unless we can demonstrate compelling legitimate grounds to continue processing.

Automated decision making/profiling – We can only carry out automated decision making under certain circumstances. If it is necessary for entering into a contract, it is authorised by law, or we have the subjects explicit consent.